TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

HACKER JOURNAL

n. 62 www.hackerjournal.it

QUATTORDICINALE ANNO 3 - 9/23 SETTEMBRE 2004 - SPED. IN ABB. POST. 70% - MILANO - IL PREZZO IN COPERTINA È VALIDO SOLO PER L'ITALIA

BLUETOOTH

CELLULARI A RISCHIO!

2€

NO PUBBLICITÀ

SOLO INFORMAZIONI E ARTICOLI

CALCOLO DISTRIBUITO

IL TEAM DI HJ!

SHOPPING DA SPIA

SU INTERNET C'È DI TUTTO

INDYMEDIA SEQUESTRATA

DOMANI A CHI TOCCHERÀ?

4ever

L'Isola dei Famosi: VOTI TRUCCATI!

40062

9 771594 577001

Anno 3 – N. 62
04/18 Novembre 2004

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Assurdolandia

"The Net - Intrappolata nella rete". Sandra Bullock fa una richiesta Whois e ottiene l'indirizzo IP di Pretorian. Inquadratura larga: si legge 75.748.86.91. Seguono inquadrature successive mentre la situazione non è cambiata. Cambiano invece i numeri Ip: 23.75.345.200, poi Whois risolve finalmente il numerico, che nel frattempo è diventato 67.234.83.345, e appare un bel dominio gms.wrld.

"Codice: swordfish". A un certo punto saltano agli occhi chiaramente due indirizzi Ip: 205.873.99.890 e 209.822.89.034.
Ok, sono finzioni cinematografiche e la privacy è salva. Ma qualche cosa di più realistico non era proprio possibile? A casa nostra l'indirizzo Ip oltre 255 non può andare, ma anche qui, si sa , la matematica è evidentemente un'opinione.
Sarebbe come fare apparire, nel film Il Colore Viola, un bigliettino appiccicato al frigorifero con scritto 2 + 2 = 5, tanto è un film e non se ne accorge nessuno...

E quel dominio .wrld? Fantastico: con tutte le possibili combinazioni di tre lettere, ne hanno scelta una assurda di quattro. Potenza della finzione.
Corriere della Sera, Unità e a ruota tutti gli altri, un paio di giorni dopo il sequestro da parte delle autorità inglesi di un hard disk contenente i siti della catena d'informazione alternativa Indymedia. Strilli indignati: "Fbi sequestra i server di Indymedia" e "...gli agenti dell'Fbi si sono presentati presso le sedi americana e inglese di Rackspace..."
FBI onnipresente? Assurdo e rischioso, almeno quanto affermarlo. Infatti la questione è un po' diversa, e ne abbiamo da leggere qui a fianco.

E allora? Allora l'informazione si fa con la conoscenza, non con l'approssimazione, tanto meno gridando quello che non si sa o non si può sapere, ancora meno costruendo fesserie che sono in evidente contrasto con le leggi naturali, la logica al primo posto. Altrimenti non si abita in un mondo umano, ma in una terra dell'assurdo.
Il posto dell'hacker in tutto questo? Ci sembra evidente. Tra quelli a cui piace pensare, non schierarsi per partito preso. Avere prima in mano tutti i termini della questione è assolutamente importante.
Solo dopo, si può sferrare l'attacco.

theguilty@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Boss: TheGuilty@hackerjournal.it

I Ragazzi della redazione europea: Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron Silvio De Pecher, Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo Elenina "menosina" Varesi

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Copertina: Daniele Festa

Publishing company: 4ever S.r.l. Via Torino, 51 20063 Cernusco S/N (MI) Fax +39/02.92.43.22.35

Printing: Roto 3

Distributore: Parrini & C. S.PA. 00189 Roma - Via Vitorchiano, 81 Tel. 06.33455.1 r.a. 20134 Milano, V.le Forlanini, 23 Tel. 02.75417.1 r.a.

Distributore per l'estero: Johnsons International News Italia Spa Via Valparaiso, 4 20144 Milano - Italia

Abbonamenti: Staff S.r.l. Via Bodoni, 24 20090 Buccinasco (MI) Tel. 02.45.70.24.15 - Fax 02.45.70.24.34 Lun. - Ven. 9,30/12,30 - 14,30/17,30 abbonamenti@staffonline.biz

Direttore Responsabile: Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

L'INFORMAZIONE sequestrata

Indymedia fa parlare di sé. Uno dei siti più contestatari e contestati del momento è stato sequestrato e poi rilasciato dalle forze di polizia internazionali. Libertà calpestata o provvedimento necessario? Leggiamo la Rete.

Agosto 2004. Un articolo sul settimanale Panorama ("C'è posta per le Br") indica la Rete come mezzo possibile e probabile di collegamento tra nuove e vecchie forze terroristiche. Che è come dire che qualcuno usa il telefono per scopi illeciti: sicuramente è così, certamente avviene ed è perfettamente comprensibile che, cogliendo sul fatto o avendo fondati sospetti che ciò avvenga in un determinato caso, le autorità intervengano per scoprire i colpevoli. Non per vietare il telefono, naturalmente.

Nell'articolo suddetto si cita anche Indymedia, un sito che fa parte di una catena internazionale di siti indipendenti e alternativi, molti dei quali legati alla cosiddetta area dei No Global. Un lecito utilizzo di sofisticate tecnologie occidentali per una forte contestazione all'occidente stesso, in molti dei suoi attuali aspetti. Benissimo e possibile. Abitiamo paesi dove è ancora possibile esprimere la propria opinione e consideriamo le contraddizioni il pane quotidiano delle democrazie. Non siamo in Cina.

UN COLPO BASSO

Il 7 ottobre, dagli uffici inglesi di Rackspace (www.rackspace.com) vengono sequestrati dalla polizia londinese gli hard disk contenenti le pagine della catena Indymedia, tra cui anche quelle italiane. Cadono come birilli una ventina di siti, sembra in modo irrecuperabile.
Leggiamo solamente qualche commento in Rete più vicino all'informazione tecnologica. Da Punto Informatico: (11/10/04) "l'FBI ha sequestrato negli uffici britannici del provider americano Rackspace su cui si appoggia Indymedia, due server o i loro hard disk, 300 gigabyte di materiale Indymedia". Su questo filone tutti gli organi d'informazione hanno cavalcato la notizia, con grande sottolineature della onnipresenza dei servizi americani che starebbero imponendo censure a tutto il mondo. Tutto da leggere Paolo Attivissimo su ZewsNews (www.zeusnews.it/index.php3?ar=stampa&cod=3428): "Innanzi tutto, molti hanno avuto l'impressione che l'FBI sia piombata in Inghilterra e abbia fatto quello che le pareva. Calma un attimo: l'FBI non ha giurisdizione nel Regno Unito. Deve chiedere alle autorità di sicurezza locali" e infatti, dopo qualche giorno la questione, guarda un po', viene ricondotta a una richiesta di un PM tutto italiano, bolognese, che ha normalmente utilizzato i canali permessi dagli accordi internazionali per condurre le sue indagini. In alcune immagini sui siti suddetti sembra fossero presenti fotografie di agenti in borghese, con tanto di didascalie contenenti minacce neppure troppo velate. Cosa fareste, se al loro posto ci foste stati voi?

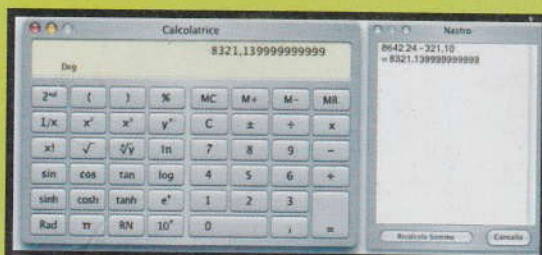
Sempre su Punto Informatico, consigliamo anche la lettura di Contrappunti "Ultima fermata: Indymedia" http://punto-informatico.it/p.asp?i=49957.
Al di là di ogni strumentalizzazione politica che è già stata innescata da tutte le parti, la confusione regna sovrana. Un atto fisico, il sequestro per una settimana, ha oscurato un organo di informazione. Di per sé un sistema di stop eccezionalmente pesante. Ma se questo, per pura ipotesi, fosse il telefono di cui sopra? Lasciamo che le indagini proseguano, cercando di comportarci civilmente nel nostro piccolo. L'inutilità di linguaggi estremi, da una parte e dall'altra, l'abbiamo sotto gli occhi tutti i giorni.

Webmaster di Indymedia: abbiamo a cuore la libertà di informazione e teniamo a che tutte le voci possano parlare. Ma sapete benissimo di essere malvisti da molti governi. Consiglio da hacker: la prossima volta siate più furbi e fate un backup. :)

ISTANBUL: TUTTO IN UNO MICROSOFT

Nome in codice Istanbul per un'applicazione che dovrebbe integrare e-mail, instant messaging, video conferenza, telefono VoiP e qualunque altro sistema di comunicazione vocale. Pronto anche a utilizzare la RingCam, webcam a 360 gradi in fase di sviluppo nei laboratori Microsoft.
Dovrebbe arrivare nella prima metà dell'anno prossimo direttamente da Microsoft. Un'altra calamita per malware?

360 GRADI IN SVILUPPO

CLAMOROSO: LA CALCOLATRICE APPLE SBAGLIATA!

La calcolatrice scientifica di Mac OS X 10.3 Panther: non ci siamo!

La calcolatrice di Windows XP: tutto ok.

Provare per credere: facciamo una qualunque operazione che coinvolga un po' di cifre dopo la virgola. Per esempio 8642,24 – 321,10. Una normale calcolatrice vi dirà che il risultato è 8321,14. Non la calcolatrice del MacOS X: il risultato sarà 8321,139999999999!
Sembra di essere tornati ai tempi dell'Intel Pentium, quando nel giugno del 1994 ci si accorse che sbagliava le divisioni! Naturalmente Apple provvede a informare i propri utenti con una bella nota tecnica che troviamo a questo link http://docs.info.apple.com/article.html?artnum=25687, consigliando di diminuire la precisione della visualizzazione e pensando di risolvere così il problema. Anzi, per dare giustificazione al tutto, tira in ballo un documento complicatissimo all'indirizzo http://docs.sun.com/source/806-3568/ncg_goldberg.html che dovrebbe dimostrare come, nei calcoli a virgola mobile, ci sia poco da fare...
Vi immaginate cosa succederebbe a usare un Apple Macintosh in una centrale nucleare o in un centro di ricerca aerospaziale? Meno male che è esplicitamente vietato nella licenza d'utilizzo del sistema operativo... ma senza andare chissà dove, vorremmo vedere la faccia di uno studente delle superiori che facendo il seno trigonometrico di 180° si trova una sfilza di cifre decimali.
Se vi serve una calcolatrice, ci dispiace ammetterlo, usate Windows!

» NON DOVREMO PIÙ RAFFREDDARE IL PC

La sostanza si chiama diboruro di magnesio ed è una polvere nerastra, che opportunamente drogata diventa un materiale superconduttore. Cosa significa? Che non dovremo più raffreddare i chip, perché la resistenza al passaggio dell'elettricità diventa praticamente nulla e non si genera calore. È un filone di ricerca che ha portato un gruppo italiano a brevettare un nuovo superconduttore che potrebbe portare alla costruzione di supercomputer mille volte più veloci degli attuali.

»SKY E DECODER

Qualcosa si muove. L'Autorità per le Garanzie nelle Comunicazioni sta esaminando le problematiche in materia di utilizzo dei decoder sui seguenti punti: possibilità di recesso da parte degli abbonati che non intendono continuare a fruire del servizio Sky con nuovi decoder; avvio delle negoziazioni con i costruttori di decoder; facilitazioni di Sky agli abbonati per le seconde abitazioni. L'Autorità ha invitato Sky Italia a formare un tavolo di confronto con le associazioni dei consumatori per esaminare i problemi connessi all'utilizzo del decoder con sistema NDS per l'accesso ai programmi televisivi via satellite. Tradotto: for-

Autorità per le Garanzie nelle Comunicazioni

Aperto tavolo di confronto tra Sky e associazione dei consumatori

HOT NEWS

SYMANTEC SI COMPORTA MALE

Non è considerata una vulnerabilità, ma poco ci manca. Daniel Milisic di Secunia ha scoperto che alcuni script di VisualBasic possono disattivare l'autoprotezione di Norton Internet Security 2004, 2004 Professional e Norton AntiVirus 2004. Così all'utente del pc non verrebbero più aperti i messaggi che notificano le attività illecite.
Per ora non ci si può fare nulla. Il popolo della rete attende ancora una risposta da Symantec, perlomeno nel momento in cui scriviamo queste righe.

INTRUSIONE DA UN MILIONE E MEZZO DI INDIRIZZI

Si è saputo solamente a fine ottobre di un'intrusione all'università della California effettuata intorno al 30 agosto. Potenzialmente attaccato un data base contenente circa un milione mezzo di indirizzi associati a numeri di carte di credito, numeri del servizio sanitario californiano e altri dati personali. Nulla si sa ancora rispetto ai potenziali danni causati e se il data base sia stato copiato in qualche altro luogo.

L'FBI sta indagando…

VIDEO DI MICHAEL JACKSON: OKKIO!

Sta arrivando un nuovo software cavallo di troia che si nasconde dietro un link pubblicizzato per email e via newsgroup. La promessa è quella di poter vedere un video riguardante Michael Jackson. In realtà si viene indirizzati su un link da cui l'unica cosa che si scarica è un trojan chiamato hackarmy, che apre una back door sul computer, rendendolo vulnerabile ad attacchi esterni.

LANCIO DEL TELEFONINO

Abbiamo mai pensato di sbattere il nostro telefonino il più lontano possibile? Ecco, il nuovo sport è proprio il lancio del telefonino. In Germania si organizzano gare vere e proprie e quest'anno il primo posto sul podio è stato raggiunto da Nico Morawa: 67,5 metri di lancio classico. Qualche immagine della gara anti-stress la troviamo al link www.handywerfen.de/ Sites/galerie2004.htm

GOOGLE SPIA PERFETTA

Il nuovo strumento di Google che consente di indicizzare il contenuto del proprio pc e di tutto quanto abbiamo prodotto, comprese le email, i messaggi e le pagine web visitate, è un sistema potentissimo per trovare contenuti sepolti nel proprio computer. L'applicazione è come "una memoria fotografica di tutto quello che possiamo avere visto sul nostro computer". Peccato che inserito in luoghi pubblici, come gli Internet Café il sistema registri inesorabilmente tutto quello che gli utenti digitano, vedono, dicono, scrivono... e l'utente successivo può tranquillamente, e in pochi secondi, vedere tutto. Account e password digitate, pagine web viste, messaggi personali inviati e ricevuti in qualunque forma...
Ovviamente si può evitare di installarlo, ma chi ci garantisce che ciò non sia stato fatto a nostra insaputa?
Lo troviamo qui: http://desktop.google.com/

se si arriverà a una accordo in modo tale che il decoder Sky possa ricevere anche i canali satellitari liberi e in modo tale che il sistema NDS possa essere adottato da qualunque produttore lo richieda. Staremo a vedere.

» DVD USA E GETTA

Si acquista, si vede e si butta. La tecnologia Flexplay consente la distribuzione di DVD a tempo, che a contatto con l'aria si autodistruggono nel giro di un paio di giorni. In 48 ore si ha tutto il tempo di guardarsi il film un paio di volte almeno e poi di gettare tutto nel cestino dei rifiuti.
I vantaggi sono immaginabili: nessuna dimenticanza di riportare il DVD noleggiato con relativi costi aggiuntivi.
Possibilità di distribuire titoli per periodi controllati, diminuzione del prezzo di vendita. Per circa 5 dollari, sotto Natale dovrebbe essere distribuito da Amazon.com il video Noel, un film che altrimenti avrebbe una scarsa diffusione se non in poche città americane. Quindi anche uno strumento molto importante per i piccoli distributori.

MAIL TO: REDAZIONE@HACKER

Come è andata con Sky

Gentile redazione, voglio comunicarvi alcuni errori che vi sono nell'articolo riguardante sky. Sky non effettua una contromisura prima di ogni partita, ma ne ha effettuata una prima della prima giornata, subito risolta e un'altra ancora da contro-battere. L'ecm non è "la chiave di decrittazione" ma sono i comandi che devono essere decrittati. Gli attacchi non avvengono prima di ogni partita e poi dove sarebbero questi "54 tipi di comandi possibili", per cui da qui a dicembre ogni partita avrà la sua contromisura"?

brithack

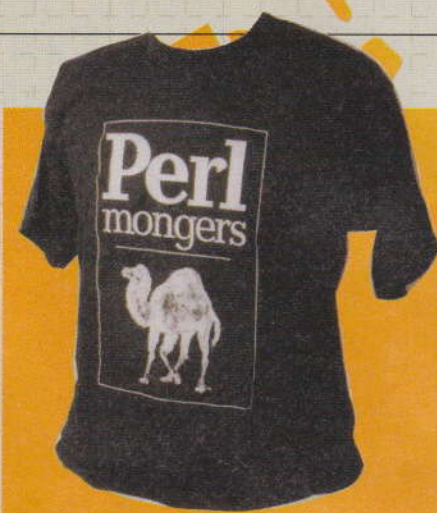
L'articolo è stato scritto il 14 settembre 2004. A quella data non era ancora possibile sapere l'evoluzione che avrebbero avuto gli attacchi. Ho lavorato di intuizione, sapendo che se i cambi dell'argo del nano fossero stati decrittati la partita successiva ci sarebbe stato un altro attacco (vedi attacchi reset sul seca1 marzo 2001 - maggio 2002).
L'imprecisione che segnali è dovuta ad una correzione che abbiamo fatto per rendere meno "criptica" quella parte dell'articolo.
I passaggio che riporti dei "54 tipi di comandi possibili" sarebbero le possibili variazioni che potrebbe subire l'argomento del nano 51. Se abbiamo fatto qualche errore nell'articolo ce ne scusiamo. Grazie per l'attenzione che hai prestato all'articolo, una critica costruttiva spesso vale 100 complimenti.

Obscuro Culto

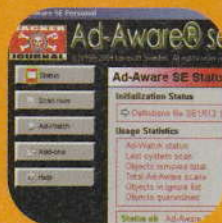
Passione Perl

Potreste indicarmi un sito in italiano da dove scaricare il linguaggio perl? Grazie
P.s.: siete forti! Andate avanti così.

Capitanbaggin

Se il problema è quello di saper scrivere in Perl, ti consigliamo, per esempio, www.html.it dove potrai trovare un tutorial per usare il linguaggio e un link http://download.html.it/recensione.asp?recensione=1310 da cui scaricare un editor perl facile da usare (ma non in italiano, ovviamente). Se vuoi Perl nella sua forma originaria, puoi sempre visitare: http://use.perl.org/articles/03/11/07/117238.shtml

Skin Hacker Journal

Servendomi del tool di sviluppo x le skin fornito da Ad-Aware ho creato una skin dedicata ad Hacker Journal! E' disponibile x il download su www.adawareskins.com /viewskin.php?id=39 in allegato la preview!
Ciao Bigthistle

Grazie e continua così! Attendiamo realizzazioni sempre più... da hacker.

LUCE USB NO

Ho seguito alla lettera l'articolo che parlava della realizzazione di una luce alimentata via USB. Non capisco perché il mio brutto anatroccolo non funziona! O meglio la luce è bassissima, ma a volte fa dei flash potenti. Sembra che la corretta alimentazione venga fornita solo quando il PC tenta di riconoscere la periferica ma cala immediatamente. Vi prego di darmi un consiglio. Grazie siete mitici.

Gabry

Non hai scambiato i fili, collegando il led (ad alta luminosità, vero?!) ai cavetti del segnale invece che a quelli dell'alimentazione? Se il cavo è fatto bene, quelli dell'alimentazione sono di diametro leggermente superiore. Comunque sono quelli collegati agli estremi esterni della presa. Prova con un tester.

LUCE USB SI

Siete formidabili!Le lampade USB del numero 60 funzionano!

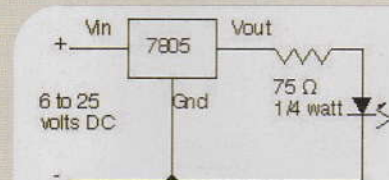
Carlo

Sicuro! :)

Luce usb così così

Ho letto l'articolo sulla costruzione della luce-USB. Confesso che da smanettone l'avevo già costruita. E' un'idea carina e utile! Volevo solo segnalare che avete dimenticato uno zero nel valore delle resistenze! Secondo la legge di Ohm devono essere 560 (oppure 440) ohm e non 56! Altrimenti nei LED (a 5 volt) circolano qualcosa come 100mA invece di 10, con la distruzione dei LED stessi!

DrWhOz

Dunque. Un led flash bianco del tipo da noi consigliato necessita circa 20 mA per dare una luce ragionevolmente buona. La tensione di lavoro di questi led è circa 3,6/4 volt (cercali, per esempio, su www.distrelec.it). Da 5 a 3,6 volt è una caduta di tensione di 1,4 volt. 1,4/0,02A = 70 ohm. Non 700. Ciao!

Luce usb in rete

Cara redazione di hackerjournal, ho letto l'articolo riguardo alla creazione di una luce attraverso la porta usb. Vorrei sapere se c'è in rete qualche sito che parla di queste cose.Siete mitici.

$$$Caino92"&%

Un salto su Google e cerca modding. Troverai pane per i tuoi denti.

Luce usb blu

Gli argomenti che preferisco sono quelli che riguardano linux, ma mi piacciono moltissimo gli articoli di modding ,di smantellamento e di piccoli apparecchi fai da te per il pc! Avevo già intenzione di costruirmi una lampada usb e il vostro articolo è capitato nel momento giusto... Visto che i led bianchi e la guaina termo restringente non li ho trovati ho usato due led blu e il cappuccio di un jack delle cuffie... Ho ottenuto una luce non molto luminosa e adatta come lampada, ma una luce rilassante e abbastanza comoda anche per la tastiera! Ora dovrò mettere un piccolo interruttore per rendere tutto più comodo. Vi allego le foto anche se sono state fatte con la web cam!

Tonino aka Jeeken

Grazie! I Led è importante che siano di tipo ad alta luminosità, di qualunque colore. Altrimenti bisogna cambiare resistenza!

Luce usb scarsina

L'articolo sull' Hacking di un cavo USB ha interessato molto me e un mio amico che abbiamo subito creato dei prototipi. Le foto allegate sono di quello scarsino che ha solo due led. L'altro ha 8 led, di cui alcuni ad alta luminosità e le foto arriveranno (forse) più avanti. Saluti.

Hexan & Decon

Bene, attendiamo anche altri esperimenti!

Soluzioni e altri argomenti

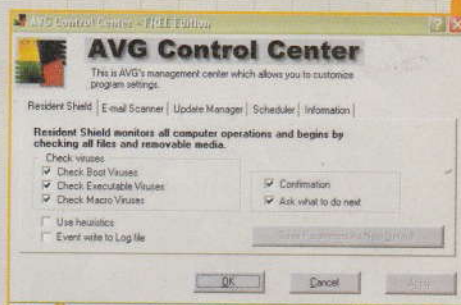
Ho letto con interesse il trafiletto che parlava dell'eco-diesel fatto "in casa": bene, io non capisco un tubo di auto o di meccanica, e non so quale impatto possa avere sull'ambiente esterno ma penso sarebbe bello continuare con argomenti simili,cercando soluzioni innovative o alternative a problemi quotidiani che esulano un poco dal campo dei computer e dell'informatica.

Luca

Ok, ne terremo conto!

Installazione avventata

Salve,
ho ricevuto in automatico (piccola icona gialla sulla barra) l'invito a installare un aggiornamento Microsoft e l'ho fatto, ma mi è parso un po' strano... tra l'altro mi indirizzava (dopo aver cliccato Si) a un sito: http://go.microsoft.com che mi pare non esista... Potete aiutarmi?? ;o(

Aiutarti per che cosa? Al massimo hai scaricato un bel trojan. Fai fare un giro sul tuo pc a SpyBot (http://security.kolla.de) e a un buon antivirus (www.grisoft.com). Toglilo dai piedi, se è riuscito a installarsi, ed evita in futuro di fare clic su qualunque cosa ti arrivi. Anzi, se hai Windows XP, installa SP2 e il suo firewall. Gli aggiornamenti seri avvengono in automatico dal sistema operativo, solo se hai settato l'opzione Aggiornamento automatico, appunto.

In Francia si può

A proposito dell'articolo "hacking del diesel", vorrei dirvi che in Francia c'è un carburante che si chiama diester ed è proprio un mix di diesel e di olio di semi di colza. Viene utilizzato soprattutto nei pullmann delle grandi città perché è molto ecologico e non sporca ! Ora lo stanno utilizzando anche nelle navi da pesca.

Frenchy

Diesel e olio di colza: NO

Caro amico Poppy, ti vorrei far sapere che un mio amico è andato avanti per qualche mese con una mistura gasolio/olio di semi. Dopo un po' però ha cominciato ad accusare alcune anomalie di funzionamento, sino allo stop definitivo della suo Opel: l'olio di semi aveva alterato le guarnizioni della pompa... Ti lascio immaginare le conseguenze!!! Ora utilizza il normale diesel, anche se si... arrabbia del prezzo più da oreficeria che da benzinaio.

Okkio quindi !!!
Per quel che riguarda l'hacking-chimico, ben venga... penso che l'unico limite dell'hacking sia la fantasia. ;-)
Ciao a tuttiGdsCrazy

Compilatore Basic (non visual)

Ciao a tutti! Volevo farvi una domanda un po' stupida: dove trovo un compilatore Basic (non Visual Basic)?
Caesar

Nessuna domanda è stupida! Prova qui: www.purebasic.com

L'isola dei FAMOSI:

Il sito Isola dei Famosi è stato hackerato: è possibile pilotare il voto di preferenza web a nostro piacimento, saltando le limitazioni imposte.

Una sera navigando senza alcuna meta precisa su Internet, siamo approdati sul sito dell'Isola dei Famosi, abbiamo conosciuto gli abitanti dell'isola, curiosato un po' qua e un po' là, e sul punto di salpare per chissà quali altri lidi abbiamo notato, non senza raccapriccio, la bella Aida Yespica fra le ultime nelle preferenze, addirittura insidiata da vicino dalla Cancellieri.

Okay che i gusti sono gusti, ma a tutto c'è un limite e così ci è venuta l'idea che forse qualcuno potrebbe "alterare" (eh, sì, abbiamo capito bene: alterare, quando ci vuole ci vuole)i risultati del sondaggio.
Da cosa nasce cosa, e abbiamo cercato di capire come potrebbe accadere. Questo è quanto ne è seguito.
Le tecniche di voto sono le consuete: si arriva sulla pagina del sondaggio, si clicca sul personaggio preferito ovvero, nel caso di Aida, si richiede la pagina www.isola.rai.it/R2_sondaggioFamoso/0,10066,342,00.html?id_risposta=1858, et voilà il gioco è fatto: abbiamo espresso il nostro voto.
Vogliamo votare ancora?
Beh, sul sito dell'isola dei famosi è possibile esprimere un'altra preferenza, ma solo dopo un'ora dall'ultima.
Okay, ma siamo sicuri che tutti si attengano a questa regola? O meglio ancora, quanto sarebbe difficile violare il controllo?
Difficile?!
Ci siamo accorti che è uno scherzo da bambini!
In realtà il controllo progettato si basa su semplici file ascii, cookie, che vengono creati dal server e scaricati sul pc: nel nostro caso durante l'operazione di voto.
Tentando di accedere nuovamente alla pagina di voto, il server verifica tramite il nostro programma di navigazione l'assenza/presenza di quei file e ci accorda, o meno, il diritto al voto.
Nel caso del sito dell'Isola dei Famosi, come detto in precedenza, è possibile votare dopo un'ora, e questo perché il server assegna ai cookie la validità di un'ora, trascorsa la quale vengono automaticamente rimossi, permettendoci di votare nuovamente.

▲ *Ecco il sito. In basso a destra possiamo dare le nostre preferenze web ai personaggi famosi. Facciamoci valere!*

IL FAMOSO DI INTERNET
1. Alessia
2. Antonella
3. Sergio
Ecco i primi tre della classifica web.

Chi è il famoso che preferisci? |vota|

Il sito della passata edizione

ININFLUENTE

Il voto su Internet non è influente ai fini della eliminazione dei concorrenti ma indica solo la popolarità dei partecipanti all'Isola dei Famosi.

VOTI TRUCCATI!

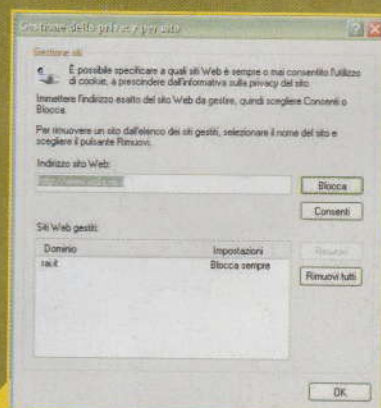
Per verificarlo basta individuare i cookie,rimuoverli e provare a rivotare o, ancora meglio, impostare il nostro programma di navigazione a non ricevere
cookie dal sito dell'Isola dei Famosi: saremo liberi di votare quante volte ci aggrada.

Okay, è già un bel passo avanti nella comprensione, ma non è ancora abbastanza: Aida è veramente in basso in classifica (a volte ci chiediamo che razza di gente frequenta il web).

Se la protezione è così labile, una soluzione ideale per chi volesse hackerare il sistema sarebbe quella di creare un semplice programma, che incrementi automaticamente i voti di Aida, mentre noi siamo liberi di navigare le pagine del sito di Hacker Journal.

Abbiamo provato se veramente possibile, scegliendo Java, ma ovviamente può essere fatto un lavoro simile in qualsiasi altro linguaggio. Del resto l'unica operazione da eseguire è quella di aprire una connessione al sito www.isola.rai.it/R2_sondaggioFamoso/0,10066,342,00.html?id_risposta=1858
senza preoccuparsi dei cookie, perché il nostro programma non vorrà essere di certo collaborativo a riguardo.
In realtà il programma creabile può essere anche un tantino più complesso. Facendo un parse della pagina HTML, ricevuta in risposta dal server, si possono rilevare, per esempio, anche le preferenze accordate ad Aida fino a quel momento, senza costringerci a ritornare al sito dell'isola per visualizzarle.
Un upgrade potrebbe essere quello di rilevare le preferenze per tutti gli altri partecipanti, ma lasciamo ogni altra considerazione ai più volonterosi!

Simone

▲ *Nella pagina dove possiamo votare, l'operazione ci sarebbe consentita solo lasciando un'ora di intervallo tra un clic e l'altro. Ma c'è chi vuole andare oltre...*

▲ *Ecco come si potrebbe fare per votare continuamente: in Internet Explorer andiamo sotto Strumenti > Opzioni Internet scegliamo Privacy > Siti e quindi impostiamo www.isola.rai.it. Un clic su Blocca e il gioco è fatto!*

HACK TEST

Hai appena finito di leggere questo articolo e:

1. **Corri sul sito dell'isola dei famosi a votare il tuo personaggio preferito barando.**
2. **Sai che, quando farai un sito con votazioni on-line, non commetterai lo stesso errore.**

RISULTATO

Se hai risposto 1 sei un lamer, se hai riposto 2, sei sulla strada giusta!

Il mistero del file spione

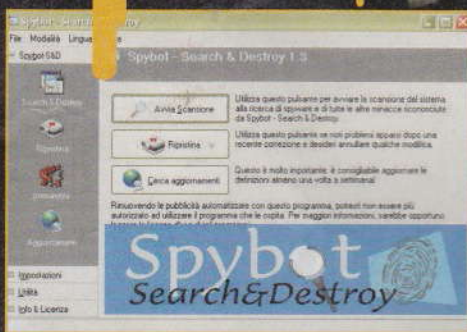
Sono sempre più frequenti le confuse segnalazioni di chi dice di vedere il proprio pc impegnato in grandi duplicazioni di file in arrivo da Internet, con grande spreco di tempo e, ovviamente, con grande sospetto per un comportamento anomalo.

Come se il nostro computer usasse dei dati della rete, e non, senza motivo. Sono perfino stati segnalati flussi di dati verso indirizzi ben precisi. Per esempio verso www.comcast.com, www.rr.com, www.bb4.org e molti altri. È normale tutto ciò? Ovviamente no, soprattutto se cerchiamo di indagare la sorgente di un comportamento così strano...

Spyware e dintorni

La prima cosa da fare, a questo proposito, è quella di cercare di individuare il colpevole del comportamento sospetto all'interno del nostro pc. Un buon software che individui e distrugga il malware può fare al caso nostro. Spybot è quello più in voga: semplice da usare, aggiornato, veloce quanto basta ed efficace su tanti fronti interni al pc, dagli eseguibili alle voci di registro.

Lo possiamo scaricare da http://security.kolla.de. Installiamolo, aggiorniamolo subito come ci viene proposto nella stessa fase di installazione ed eseguiamo una scansione di tutto. Se è presente uno spyware abbiamo risolto il problema e possiamo distruggerlo con lo stesso Spybot. Dopodiché dovremo anche chiederci come ha fatto a entrare e cercare di mettere a fuoco tutte le falle del sistema, o nostri comportamenti a rischio negli ultimi tempi. Probabilmente un po' di questi problemi potremmo facilmente risolverli applicando un firewall software. Oppure, considerato che siamo utenti Windows e quindi pronti ad accettarne le conseguenze, è la volta buona che scarichiamo il Service Pack 2, che di firewall ne ha internamente uno piuttosto efficiente.

Comunque sia, se abbiamo Windows XP, proviamo a installare SP2 e la sua brava patch da poco apparsa. Un pacco Microsoft, certamente, ma il minore dei mali rispetto alle versioni passate. Perlomeno aumenta visibilmente la stabilità del sistema.

Un classico anti spioni: Spybot all'attacco

NDISUIO.sys

Se queste procedure però non bastano, perché non viene segnalata la presenza di spyware e sembra tutto regolare, la nostra attenzione può concentrarsi su qualche specifico file presente nello stesso sistema operativo. NDISUIO.sys è uno di questi.

A detta di molti utenti e di discussioni su diversi forum, il traffico irregolare di dati internamente alla nostra macchina pare sia generato proprio da questo file.

In effetti NDISUIO.sys è un driver Microsoft, e non uno spyware. O perlomeno così viene descritto. Alcuni invece affermano che potrebbe esserci qualche versione di questo file un po' troppo spiona, e che varrebbe comunque la pena disattivarlo.

Altri sono convinti che se questo file 'diventa' spione, è tutta colpa di qualche malware, non ancora individuato, che altera un normalissimo driver Microsoft che, di per sé, non avrebbe nulla del Grande Fratello.

Quindi, che fare?

Microsoft descrive il servizio a questo indirizzo:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wceddk40/html/cxrefndisuser-modeiodriver.asp dove, in pratica, dice che NDIS User-mode I/O (NDISUIO) è un driver di protocollo che

CHI VUOLE PROVARE?

La soluzione al mistero di NDISUIO.sys non è facile, ma per i più curiosi un sito da cui iniziare è almeno questo:
http://www.ndis.com/pcakb/KB01010301.htm
Se invece si vogliono leggere delle esperienze di utenti al proposito, eccole qui: http://forum.defcon.org/archive/index.php/t-2142.html

Mentre si usa Windows XP può capitare che il flusso dei dati da e per la rete aumenti vertiginosamente. Cosa sta succedendo?

supporta l'invio e la ricezione dei dati via Ethernet utilizzando ReadFile e WriteFile. Come driver di protocollo, NDISUIO dice come stabilire la comunicazione tra i controllori della rete Ethernet, come adeguare i filtri di pacchetto e come ricevere e inviare i dati.
Ecco alcune delle cose che possono fare con il driver NDISUIO:

▲ *Disattiviamo NDISUIO.sys intanto che siamo in tempo*

- autenticazione utenti per i dispositivi WiFi 802.11
- recupero dei valori della potenza del segnale
- invio e ricezione di pacchetti attraverso le porte di collegamento
eccetera eccetera.

Quindi un vero generatore di flussi di dati, soprattutto utilizzato se attiviamo la comunicazione WiFi.

E se non la utilizziamo? Allora possiamo disattivarlo, a scanso di equivoci.

Come disattivare il file

Ecco la procedura per disattivare il servizio NDISUIO.SYS:

Start -> Esegui -> Regedit -> OK

Si aprirà l'editor del registro di sistema. Cerchiamo la chiave:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ndisuio

Cambiamo il valore di "Start" da

0x00000003 a 0x00000000

Riavviamo il sistema.

Come riattivarlo.

Procedura per attivare il servizio NDISUIO.SYS:

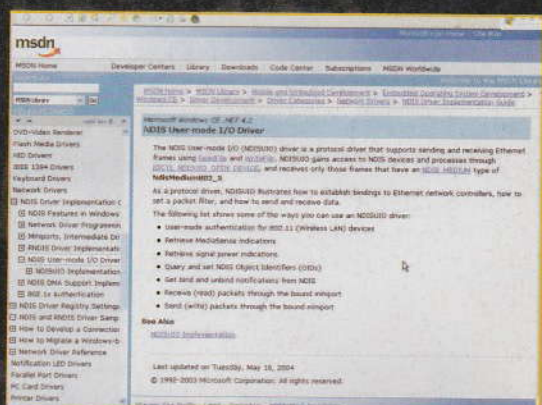
Start -> Esegui -> Regedit -> OK

Si aprirà l'editor del registro di sistema. Cerchiamo la chiave:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ndisuio

Cambiamo il valore di "Start" da

0x00000000 a 0x00000003

Riavviamo il sistema.

▲ *Sul sito Microsoft troviamo descritta (in inglese) la funzione di NDISUIO.sys*

Utilizzando questo metodo il driver NDISUIO.sys non è più attivo e quindi non genera più traffico, risparmiando tempo macchina e, se coinvolgeva Internet, anche banda per i nostri usi e consumi. Abbiamo provato qualche funzionalità di Windows, anche "Aggiornamenti Automatici", e questa disattivazione sembra non creare alcun problema. Purtroppo la disattivazione di NDISUIO.sys non permette l'utilizzo di sistemi Wireless.

Da una segnalazione di Kappa

Bluebugging, il nuovo incubo per i telefoni Bluetooth!

Se pensavamo che i dialer fossero un problema solo per i telefoni fissi, allora non abbiamo mai avuto a che fare con il Bluebugging.

Immaginiamo di potere controllare un telefono altrui, come se fosse connesso al nostro notebook, esattamente come facciamo con il nostro telefono.
Risultato: telefonate a scrocco, massiccia invasione della privacy e nel futuro anche qualche acquisto a spese altrui.

Se poi pensiamo che tutto questo è possibile adesso, anzi da più di sei mesi, allora potremmo essere di fronte ad uno dei maggiori scandali che abbiano mai travolto la telefonia.
Ma andiamo con ordine, ad iniziare dal vocabolario.
Esistono tre tipi diversi di interazione che si possono avere con un telefono Bluetooth (altrui):

Bluejacking

Ovvero l'invio di messaggi il cui contenuto è interamente nel campo nome.
In questo modo il messaggio viene visualizzato sul telefono dell'obiettivo. In Inghilterra viene usato normalmente come approccio sessuale e molti ragazzi e ragazze rendono volontariamente possibile questa connessione per il brivido dell'avventura.

Black Hat: sul tavolo tutto il necessario alla demo, ma in realtà basta un notebook e un dongle bluetooth

Bluesnarfing

Noto dal Novembre 2003, scoperto da A L Digital. È possibile copiare i dati di un telefono: il registro delle chiamate, la rubrica, il codice IMEI, l'agenda e le foto; possibilità di "aggiornare" i dati sul telefono obiettivo.

Bluebugging

Divulgato da Martin Herfurt nel marzo 2004, in occasione del CeBIT di Hanover. È possibile creare una connessione non autorizzata attraverso il collegamento seriale. Accesso completo al set AT del telefono: ovvero si possono mandare SMS, eseguire telefonate e programmare il telefono.
Le conseguenze di questo sono molto chiare per tutti.

I due relatori a DefCon sono stati Adam Laurie <adam@algroup.co.uk>, capo della sicurezza presso al A L Digital, e The Bunker e Martin Herfurt <martin.herfurt@salzburgresearch.at>, responsabile Ricerca e Sviluppo presso il Salzburg Research Forschungsgesellschaft mbH. Hanno entrambi intravisto la possibilità di gestire i telefoni bluetooth a scapito dell'utente, e correttamente hanno scritto un avviso sul forum degli sviluppatori bluetooth. Per due settimane non è successo nulla, allora hanno pubblicato il tutto sul sito di Slashdot; risultato: Nokia si è messa in contatto con loro due giorni dopo.

▲ *Martin Herfurt, a sinistra, e Adam Laurie durante il loro intervento a BlackHat.*

Comunque tutte le aziende sono state informate ed è interessante vedere quali siano state le loro risposte riguardo le vulnerabilità scoperte dagli autori:
Nokia: ha immediatamente contattato gli autori.
TDK (sviluppa componenti per cellulari): ha pubblicato un documento che spiega che questo non è possibile.
SonyEricsson: ha contattato gli autori e poi ha pubblicato un documento che spiega che questo non è possibile.
Siemens e Motorola hanno mandato degli esemplari dei nuovi telefoni agli autori per verificarne la non vulnerabilità.

Se avete dubbi sulla reale possibilità di telecontrollare un telefono bluetooth, sappiate che io ho avuto la possibilità di assistere alla dimostrazione sia a Black Hat, sia a DefCon. Gli autori armati di notebook e dongle bluethoot hanno inizialmente controllato il telefono di un loro "complice" seduto in quarta fila, che poi si è alzato per passeggiare nel corridoio, permettendo a tutti i presenti di ascoltare le sue conversazioni. Successivamente hanno mandato SMS verso il loro telefono inquadrato dalla telecamera, da un altro telefono sempre di un "complice" (per non commettere un reato).

IN PERICOLO

Ecco la lista dei telefoni possibilmente soggetti a Bluesnarfing e Bluebugging:

Marca	Modello	Firmware	Backdoor	Bluesnarfing in modalità Discoverabe	Bluesnarfing in modalità NON Discoverabe	Bluebugging
Ericsson	T68	20R1B 20R2A013 20R2B013 20R2F004 20R5C001	?	Yes	No	No
Sony Ericsson	R520m	20R2G	?	Yes	No	?
Sony Ericsson	T68i	20R1B 20R2A013 20R2B013 20R2F004 20R5C001	?	Yes	?	?
Sony Ericsson	T610	20R1A081 20R1L013 20R3C002 20R4C003 20R4D001	?	Yes	No	?
Sony Ericsson	T610	20R1A081	?	?	?	Yes
Sony Ericsson	Z1010	?	?	Yes	?	?
Sony Ericsson	Z600	20R2C007 20R2F002 20R5B001	?	Yes	?	?
Nokia	6310	04.10 04.20 4.07 4.80 5.22 5.50	?	Yes	Yes	?
Nokia	6310i	4.06 4.07 4.80 5.10 5.22 5.50 5.51	No	Yes	Yes	Yes
Nokia	7650	?	Yes	No (+)	?	No
Nokia	8910	?	?	Yes	Yes	?
Nokia	8910i	?	?	Yes	Yes	?
* Siemens	S55	?	No	No	No	No
* Siemens	SX1	?	No	No	No	No
Motorola	V600 (++)	?	No	No	No	Yes
Motorola	V80 (++)	?	No	No	No	Yes

* Modelli non vulnerabili
++ Il V600 e il V80 sono in modalità discoverable automaticamente per 60 secondi quando vengono accesi o si seleziona questa funzione da menu. Motorola ha comunicato che le nuove versioni del firmware non avranno questo problema.
Fonte dei dati : http://www.thebunker.net/release-bluestumbler.htm

Se per i dialer si è arrivati in ritardo, cosa vogliamo fare per il controllo dei telefoni bluetooth? Circa il venti percento dei telefoni attualmente in produzione è vulnerabile il che vuole dire che un malintenzionato, per esempio stando comodamente seduto ad un tavolo del bar della stazione Termini a Roma con il suo notebook con dongle bluetooth, può agganciare giornalmente circa 200 telefoni vulnerabili e farli chiamare un numero 899xxxxxx da 5 euro a chiamata, con un reddito giornaliero di 1.000 euro! Tra l'altro la connessione bluetooth non lascia tracce nei log del telefono e data la non duplicabilità dei telefoni GSM (anche qui ci sarebbe MOLTO da dire) i poveri sfortunati non dovrebbero fare altro che pagare la salatissima bolletta!

Laurie afferma che la maggior parte delle persone si scorda di spegnere il Bluetooth ed il discoverable mode dopo che hanno scambiato delle informazioni con una periferica (ad esempio chi usa una cuffia o un sistema viva voce in macchina). Circa il venti percento dei telefoni "scoperti" in giro erano visibili e vulnerabili a qualche tipo di attacco. In una prova di due ore fatta a Londra durante l'ora di punta, Laurie ha trovato 336 telefoni bluetooth, 77 dei quali vulnerabili.

COLLEGAMENTI:

http://agentsmith.salzburgresearch.at/
http://www.thebunker.net/release-bluestumbler.htm
Matthew Byng-Maddick <mbm@aldigital.co.uk>

Silvio De Pecher

TUTTI nell'HJTeam!

Vogliamo creare squadre di calcolo distribuito sotto il nome di Hacker Journal? Le sfide possibili sono talmente tante che di difficile c'è solo scegliere!

L'idea è semplice e vincente. Tutti noi usiamo il computer come il nostro cervello, al dieci per cento delle sue capacità. Allora, perché non prestare il tempo macchina sprecato del computer a progetti utili e/o divertenti?

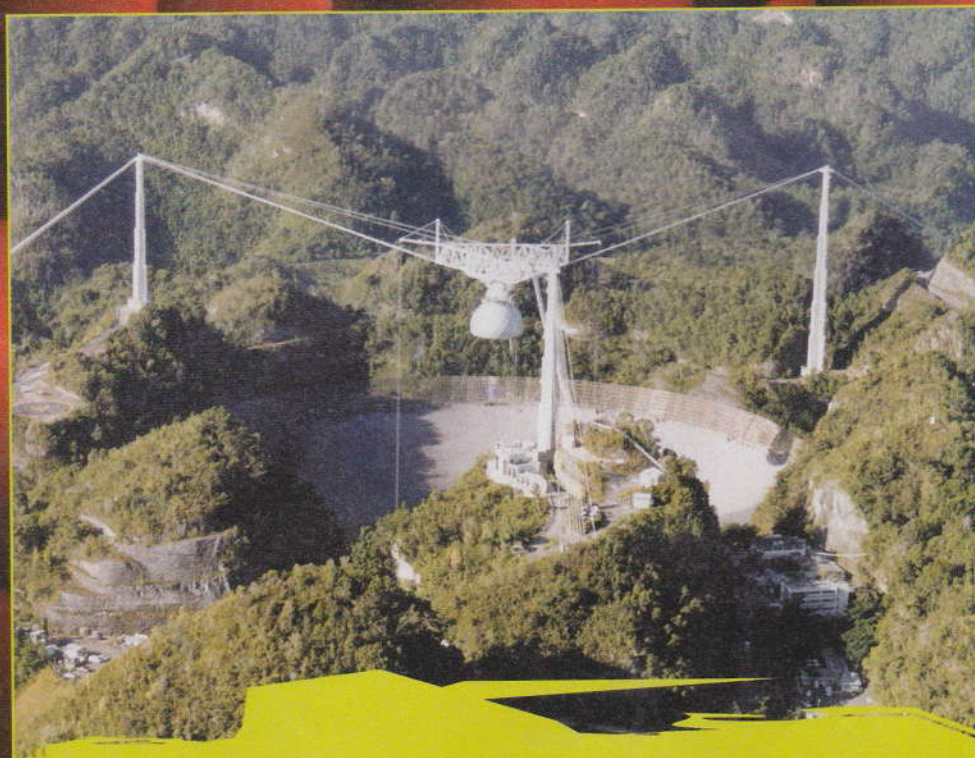
È la cosa più hacker che possa esserci. Condivisione delle conoscenze e delle risorse, globalità del sapere, formazione di comunità, mettersi in modo disinteressato al servizio di una buona causa.

Di più. Visto che spesso in questi progetti si possono formare gruppi, che competono per ottenere i migliori risultati, perché non fondare degli HjTeam? I team possono essere anche più di uno, con nomi diversi. Chi ne fonda uno ci avvisi! Lo pubblichiamo sulla rivista e gli facciamo pubblicità.

Qui sotto ci sono un po' di progetti cui si può partecipare. Ce ne sono molti altri, naturalmente. Attendiamo le segnalazioni!

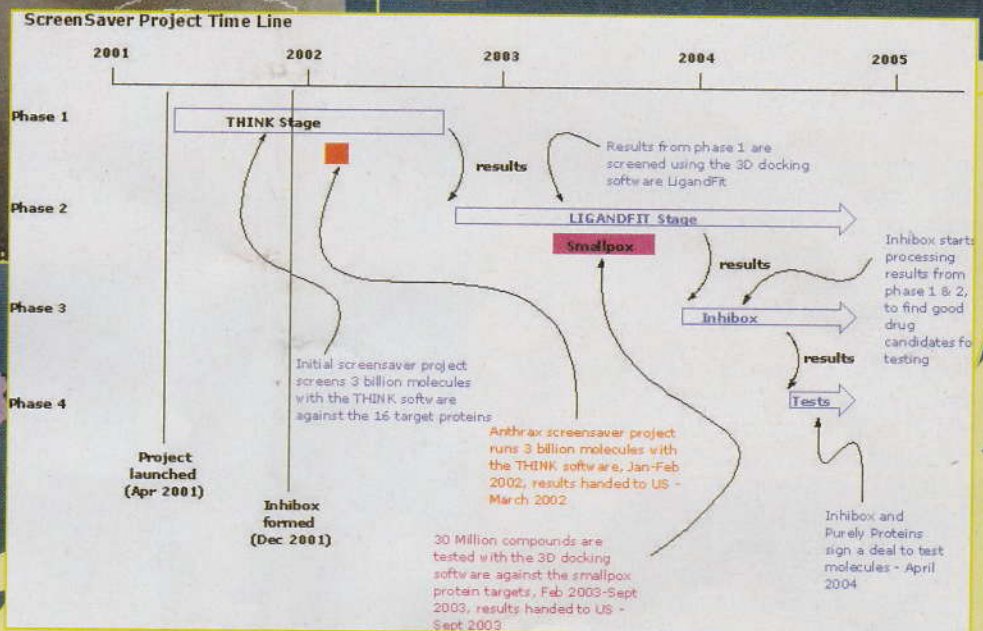
Alcuni progetti di computing distribuito

Trovare gli extraterrestri

Il progetto SETI@home è uno dei più longevi. I client analizzano dati radio captati dal grande radiotelescopio di Arecibo e cercano segnali che possano provenire da intelligenze aliene. C'è chi ci crede alla follia e chi è scettico. A ognuno la sua posizione.
Fascino: galattico. Utilità: Boh. Software: http://setiathome.ssl.berkeley.edu/.

DIECIMILA BUONE RAGIONI PER ANDARE A CACCIA DI NUMERI

Lo **scorso 27 aprile RSA ha assegnato un premio di diecimila dollari** (quasi altrettanti euro) a un gruppo di ricercatori che ha usato una rete di cento computer per tre mesi allo scopo di scovare due numeri primi. Dai due numeri ne erano stati generati altri otto, fondamentali per la cifratura RSA a 576 bit. Scovare i numeri cercati significa che la solidità della cifratura non è sufficiente e che bisogna lavorare con numeri ancora più alti. Il gruppo comprendeva ricercatori da Germania, Olanda, Regno Unito, Canada e USA. A pagina 28 spieghiamo come vincere centomila dollari…

QUANTO E' POTENTE UNA RETE DI CALCOLO DISTRIBUITO

Secondo i responsabili di distributed.net, la rete di computing formata da persone che aderiscono liberamente al progetto prestando tempo macchina dei loro computer è equivalente a 160 mila Pentium II a 266 MHz che lavorano 365 giorni l'anno 24 ore su 24. Compresi i bisestili. :-)

Il grande radiotelescopio di Arecibo, Portorico. Raccoglie i segnali che vengono elaborati dal progetto SETI@home.

▲ *Lottare contro il cancro con un salvaschermo? Si può. Mica ci sono solo le arance della salute.*

Piegare le proteine

In biologia è tuttora un mistero come le proteine si assemblino o, nel gergo degli scienziati, si ripieghino prima di entrare in funzione (se non lo fanno nel modo corretto sono guai). Folding@home esegue in rete i complessi calcoli per decidere come si piegherà una certa proteina.
Fascino: molecolare: Utilità: Panacea. Software: http://folding.stanford.edu/download.html

Trovare la cura contro il cancro

L'Università di Oxford cerca tempo macchina in tutto il mondo per verificare l'efficacia di oltre tre miliardi e mezzo di molecole diverse nella lotta contro il cancro. Anche noi possiamo dare un mano, meglio: il salvaschermo.
Fascino: farmaceutico. Utilità: Totale. Software: http://www.chem.ox. ac.uk/cancer/download.html.

Sapere che tempo farà

Il più grosso esperimento mai tentato prima di produzione di previsioni del tempo per il XXI secolo.

Da vedere è bellissimo, perché praticamente ogni client genera una sua previsione di come cambierà il tempo nei prossimi anni. Fascino: D'atmosfera. Utilità: Assai più di un ombrello. Software: http://climateapps2.oucs.ox.ac.uk/cpdnboinc/index.php.

ANCORA PIU' PROGETTI

All'indirizzo http://www.aspenleaf.com/distributed/distrib-projects.html si trova una lista aggiornata di progetti di computing distribuito in corso. Sono più di venti, dalla craccatura dei cifrari al genoma umano alle previsioni del tempo…

PENTIUM A 6 GHZ!

Il nostro pc è stato progettato con dei limiti. Che noi vogliamo superare. Uno dei principali problemi è il calore generato dai componenti, il processore primo fra tutti. Se lo facciamo funzionare ai valori dichiarati dalla casa costruttrice, stiamo usandolo come tutti: siamo nella media. Ma noi vogliamo di più, non possiamo accontentarci. E tutti i componenti, si sa, non sono mai fatti funzionare al limite delle loro capacità. Invece noi vogliamo spingerci oltre ogni limite.

Abbiamo tutti presente il rumore che fa il nostro pc quando è acceso: sono le ventole di raffreddamento. Tutti i componenti elettronici scaldano. Ciascun componente che si mette dentro un processore scalda. E oggi, in un processore moderno, si parla di qualcosa come 1 miliardo di transistor in circa 2 cm quadri di scheggia. Quindi se lasciamo il nostro processore senza raffreddamento, brucia.

A maggior ragione se schiacciamo sull'acceleratore e spingiamo il nostro processore a lavorare oltre i limiti dichiarati. È così che i tentativi di oltrepassare ogni barriera sono spuntati come funghi. Con quali risultati? Beh, guardare per credere. C'è chi ha veramente superato ogni confine: un Pentium 4 fatto girare a oltre 6 GHz è l'attuale record assoluto. Una barriera che sembrava impossibile.

Il problema principale è quello di raffreddare la CPU con un sistema che riesca a smaltire il più velocemente possibile il calore prodotto. Questo vuole dire crea-

▲ *Il vero record assoluto: 6 GHz grazie all'azoto liquido! (by Macci, del team Akiba, www.akiba-pc.com)*

SE VOGLIAMO PROVARE

Beh, se il nostro scopo è quello di evitare un po' del rumore delle ventole che raffreddano i moderni processori, non è consigliabile adottare misure così estreme come il ghiaccio secco o addirittura l'azoto liquido.

Possiamo essere più che soddisfatti di utilizzare sistemi di raffreddamento più classici, che funzionano sul principio dei radiatori dell'acqua nelle automobili. Viene fatta circolare dell'acqua, o un liquido refrigerante, dentro una serpentina e sopra il processore. Il liquido assorbe il calore generato e lo smaltisce nella serpentina, che in genere è raffreddata anche lei da una ventola, mantenuta però a un numero di giri così basso che il rumore è impercettibile. In questi casi è bene usare un sistema di raffreddamento che preveda l'assorbimento del calore sia sul processore, sia sugli altri componenti principali della scheda madre. Un buon esempio lo

L'overclocking estremo è arrivato a mettere il Pentium nel-l'azoto liquido. Ecco qualche immagine e qualche soluzione più abbordabile.

▲ Il problema è il raffreddamento di tutto ciò che sta vicino: un esperimento da far durare poco... (foto Tom'sHardware, www.tomshw.it)

CPU raffreddata ad azoto liquido, ma gli altri chip hanno bisogno di un raffreddamento almeno ad acqua.

troviamo da www.elma.it/cpufan/coolriver1.htm, ma una ricerca su Google ci darà una panoramica decisamente grande. Attenzione comunque alla rumorosità.
Se è proprio il fattore rumore che ci spinge a raffreddare il nostro pc con sistemi alternativi, possiamo prendere in considerazione questo kit: www.zalman.co.kr che non prevede nessuna ventola ed è pure bello da vedere, anche se, ovviamente, un po' ingombrante!

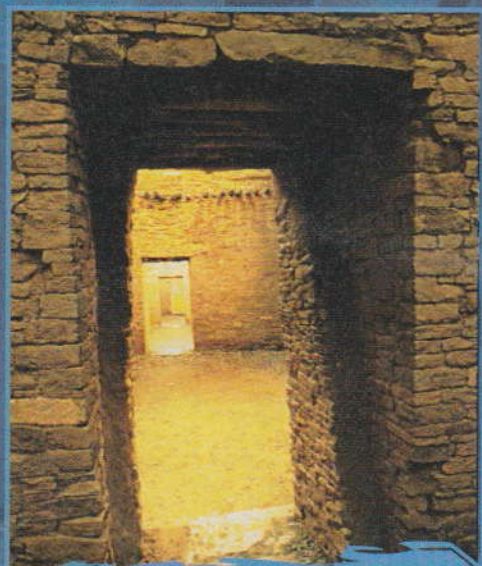
re una differenza di temperatura tra l'interno e l'esterno del processore quanto più alta possibile. Ovvero trovare un sistema di raffreddamento alla temperatura più bassa che riusciamo a produrre.
I primi tentativi sono stati fatti con l'anidride carbonica solida, il cosiddetto ghiaccio secco. Il ghiaccio secco passa direttamente dallo stato solido a quello gassoso raggiungendo temperature di -78 gradi. Usare materiali a queste temperature non è facilissimo. I problemi che possono sorgere anche solamente con il ghiaccio secco sono:
a) **la difficoltà di maneggiarlo.** Indispensabili dei guanti che resistano a temperature così basse, perché toccarlo con le mani provoca ustioni profonde e la pelle si incolla, letteralmente, alle superfici così fredde;
b) **è necessario continuare ad aggiungere ghiaccio secco al sistema, perché sublima velocemente.** Un Pentium scarsino e in condizioni normali, a 2,2 Ghz, dissipa già circa quanto una lampadina da 60 Watt, e quindi il nostro ghiaccio secco si consuma in fretta. Anche perché raffredda anche l'ambiente circostante, che contribuisce al consumo;
c) **in un ambiente un po' umido il ghiaccio secco genera brina e l'acqua presente nell'aria ricopre la componentistica presente sulla scheda madre.** Questo può causare abbassamenti della resistenza tra punti diversi, se non proprio cortocircuiti. Quindi è bene stare attenti a isolare accuratamente la zona. In più aumenta sia la corrosione delle parti metalliche (per esempio i pin dei circuiti), sia lo stress meccanico a cui i componenti sono sottoposti.
Un metodo è illustrato al link www.hwtweakers.net/postt1369.html
Se vogliamo procurarci del ghiaccio secco, possiamo provare presso www.dryce.it, che ha diversi rivenditori in tutta Italia.
Tramite il raffreddamento a ghiaccio secco c'è chi è riuscito a ottenere un overclocking del processore di circa 1 Ghz, arrivando quindi a qualcosa intorno ai 4 Ghz.

Sempre più giù

Se riusciamo ad abbassare ancora la temperatura, possiamo abbattere altre barriere. Ma qui le cose si complicano non poco e la faccenda diventa più da laboratorio universitario che da overclocking casalingo. Se non altro per le sostanze in gioco. La possibilità più semplice per abbassare drasticamente la temperatura è infatti quella di usare l'azoto liquido. Venduto in fiasche termoisolate, i vasi di Darwin o "thermos", è l'ultima barriera dell'overclocking perché raggiunge la bellezza di circa 196 gradi centigradi sotto zero! Grandi esempi di sperimentazioni in questo senso le troviamo qui www.akiba-pc.com/article.php?34.0, dove è stato battuto il record assoluto di overclocking, portando da 3,2 a oltre 6 Ghz la frequenza di funzionamento di un Pentium 4!
E se vogliamo divertirci a guardare un esperimento completo, e filmato, di queste prove, allora dobbiamo scaricare subito il grandioso filmato all'indirizzo www.de.tomshardware.com/guides/cpu/20031230/images/thg_video_11_5ghz.zip che è l'esperimento tentato, e riuscito, di superare i 5 Ghz fatto dagli appassionati di Tom's hardware, la cui versione italiana troviamo all'indirizzo www.tomshw.it e da cui abbiamo tratto le foto che vi facciamo vedere.
Per guardare il filmato è indispensabile avere installato un codec DivX, che scarichiamo gratuitamente all'indirizzo www.divx.com/divx/download.
Segnaliamo che anche il team italiano ha tentato di entrare nel primato: tutti i particolari all'indirizzo www.tomshw.it/howto.php? guide=20040610.

▲ Una piovra di raffreddamento... (foto Elma)

Attacco al wat

Si può veramente proteggere una fotografia digitale? La verità è che ...

Sulla pagina http://www.petitcolas.net/fabien/watermarking/image_database/index.html si trovano molte foto valide per provare la validità delle filigrane digitali.

Questa foto è proprietà di Robert E. Barber, Barber Nature Photography (REBarber@msn.com).

Internet è il disastro del copyright, lo sappiamo. Ma non sono solo di film o musica. Una delle piraterie più diffuse è quella delle immagini. Si può pensare bene o male del copyright, ma è indubbio che i disegnatori vivano disegnando. Per cui cercano vie per difendere il loro lavoro dall'utilizzo non autorizzato. Più che altro, non retribuito.

Il watermarking serve a evitare che una immagine digitale venga modificata per renderla diversa dall'originale e spacciarla su Internet abusivamente.

Le tecniche base

All'inizio gli artisti inserivano le informazioni di copyright nell'intestazione (header) dei file. Peccato che registrando il file in un altro formato esse spariscano. Quelli senza scrupoli addirittura cambiano lo header originale con il loro.

Un metodo più astuto consiste nel sovrapporre all'immagine un'altra immagine, trasparente, che funge da filigrana. Disgraziatamente un ladro molto abile è capace di separare le due immagini, a costo di molta fatica. Per un professionista del furto ne vale la pena.

Infine c'è chi ricorre ai programmi di filigrana digitale. Quasi tutti codificano i dati di copyright sotto forma di motivi invisibili dentro l'immagine. Il problema è che non devono disturbare l'immagine stessa e, allo stesso tempo, resistere alla manipolazione.

Un altro metodo molto usato dai ladri è il cosiddetto mosaico. Si prende una

ermarking

IL WATERMARKING

...la filigrana. Come quella che si vede guardando controluce una banconota. Informazione interna all'oggetto, non cancellabile e falsificabile con una certa difficoltà. Nel mondo digitale il watermarking indica, per esempio, la marcatura invisibile dei file grafici creati con Photoshop ed equivalenti. La filigrana digitale dovrebbe restare riconoscibile anche se il documento viene stampato e fotocopiato però, insomma, dipende.

QUALE delle DUE FOTO è QUELLA VERA?

Su http://www.ctr.columbia.edu/~cylin/auth/authresult1.html si vede un esempio di come un software può riconoscere le aree in cui una foto è stata truccata e individuare un falso.

immagine e la si affetta in tanti pezzi. Poi si ricostruisce l'immagine sul Web con una tabella HTML, ogni cella della quale contiene un pezzo dell'immagine. Per il resto, i ladri sfigati (la gran parte) si arrangiano con ricampionamenti e ridimensionamenti dell'immagine. Il problema è proprio questo: per sconfiggere molte filigrane anche questi trucchetti da poco sono sufficienti.

Programmi di testing (per modo di dire) o di difesa

Uno dei più famosi programmi disponibili per testare la solidità di una filigrana digitale è StirMark di Fabien A. P. Petitcolas, reperibile a http://www.petitcolas. net/fabien/watermarking/stirmark/index.html. Secondo l'autore, StirMark è in grado di rilevare e alterare le filigrane di numerosi sistemi specializzati, come Digimarc, EIKONAmark, EPFL, JK_PGS, PictureMarc, Pretty Good Signature, SureSign di Signum Technologies e SysCop. Ovviamente questa tecnologia è concepita solo per dimostrare l'inadeguatezza delle tecniche correnti e non va usata per cancellare filigrane, come l'autore sottolinea sul sito.

Su http://www.stealthencrypt.com si trova il software Stealth Encryption, che vuole fare un passo avanti mescolando insieme cifratura e steganografia. Le informazioni di copyright vengono inserite in modo invisibile nell'immagine e cifrate a 128 bit con una password scelta dall'artista.

Tutta questione d'immagine

Qualcuno sarà dalla parte degli autori, qualcuno no. Qualunque posizione abbiamo, è indubbio che questa continua lotta tra guardie e ladri (sempre tra virgolette) continuerà con tecnologie sempre più impressionanti per ingegnosità.

UNA MAILING LIST E BEN DI PIU'

Copyright di Gerald Deshais, Department of Materials Science & Metallurgy, University of Cambridge.

Particelle di idrogeno dentro una lega di alluminio, magnesio, rame e zinco.

Interessati al tema? Un posto dove trovarsi è la mailing list Watermarking World, a http://www.watermarkingworld.org/ml.html.
Su http://www.networkmagazineindia.com/200108/security1.htm si trova un buona introduzione con un glossarietto. Infine consigliamo sicuramente la lettura del Pdf presente a http://www.petitcolas.net/fabien/publications/ih98-attacks.pdf e un'occhiata al sito http://www.jjtc.com/stegoarchive/stego/watermrk.html, contenente i link a un gran numero di programmi di watermarking.
Anche http://www.wowarea.com/english/help/stega.htm contiene un sacco di risorse utili.

Copyright del Signal and Image Processing Institute dell'University of Southern California.

I SEGRETI del OVERFLOW

Una delle tecniche di attacco più praticate, devastanti e pericolose

Il buffer overflow è diventato uno dei rischi di sicurezza più grossi che esistono su Internet e nelle reti locali. È così diffuso perché gli errori di programmazione accadono spesso e non è difficile commetterne uno di questo tipo. Non sempre si ha accesso al codice sorgente, che permetterebbe di individuare il problema, e non sempre chi ha il codice sorgente sa che cosa farsene. Per fortuna siamo qui noi!

Avvertenza: serve capire almeno un pochino di linguaggio C. Una buona occasione per impararlo! Una guida breve ma valida, in italiano, si trova a http://programmazione.html.it/c/. Bisogna anche sapere qualcosina di hardware. I nostri esempi si riferiranno all'architettura x86, su cui si basano tutti i PC Windows.

Non era previsto

Sfruttare un buffer overflow vuol dire inviare come input al computer bersaglio più informazioni di quelle che questo è preparato a ricevere. I dati in sovrappiù vanno a sovrascrivere aree di memoria non previste e, se l'attacco riesce, vengono eseguiti dal processore.

Per capire come succede tutto questo occorre sapere come è organizzata la memoria RAM e, tanto per iniziare, che cosa sono le pagine.

Tutto è relativo (specie l'indirizzamento)

Una pagina è una parte di memoria che usa un suo schema di indirizzamento relativo. Indirizzamento relativo vuol dire che il kernel (la parte fondamentale del sistema operativo) destina la pagina a un certo processo in esecuzione, ma non sa dove risiede esattamente la pagina, ossia su quali chip di RAM vengono davvero

▲ Una immagine JPEG maligna ed ecco che parte un attacco di buffer overflow.

BUFFER

PAROLE DA SAPERE

Stack: Struttura di dati in cui le informazioni sono accessibili nel cosiddetto schema LIFO, che sta per Last In First Out, ossia l'ultimo che è arrivato è il primo ad andarsene. Lo Schema LIFO è come una pila di libri dentro uno scatolone: si può accedere solo al primo degli oggetti, quello in cima. Un'istruzione push mette un oggetto sopra lo stack, una pop lo toglie. Quasi tutti i processori hanno uno stack.

scritti i dati. La memoria per i processi è divisa in tre: segmento codice, segmento dati e segmento stack.

Nel segmento codice si trovano istruzioni in assembler (il linguaggio parlato dal processore), che vengono eseguite. L'esecuzione non è necessariamente lineare. Possono esserci salti. Per questo esiste un valore chiamato puntatore alle istruzioni. Il puntatore contiene l'indirizzo di memoria dove si trova la prossima istruzione che verrà eseguita.

Il segmento dati ospita lo spazio per le variabili e per i buffer dinamici. Il segmento stack, infine, viene usato per passare argomenti alle funzioni e per immagazzinare le variabili delle funzioni stesse. La base dello stack di solito si trova alla fine della memoria virtuale indirizzata dalla pagina. Il comando assembler pushl aggiunge informazioni in cima allo stack e il comando popl toglie quello che sta in cima allo stack per inserirlo in un registro del processore. Come per il segmento codice abbiamo anche qui un puntatore; il puntatore di stack indica dove si trova la cima dello stack.

Facente funzioni

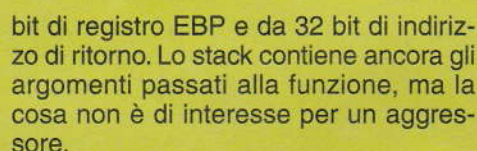
Una funzione è un pezzo di codice che si trova nel segmento codice ed esegue un certo compito, dopo di che l'elaborazione prosegue con il resto del codice. Questo è un esempio molto banale di funzione in assembler:

► *Gdiplus.dll: una libreria usata anche per programmarsi uno Space Invaders in C*

```
INDIRIZZO       CODICE
0x8054321       pushl $0x0
0x8054322       call
                $0x80543a0
                0x8054327 ret
0x8054328       leave
...
0x80543a0popl   %eax
0x80543a1       addl
                $0x1337,%eax
0x80543a4       ret
```

▲ *Molti apparecchi di rete incorporano controlli per scongiurare il pericolo di buffer overflow.*

Con l'istruzione pushl viene messo uno zero sullo stack, da usare come variabile argomento della funzione, che viene chiamata da call. La funzione prende la variabile dallo stack via popl e, dopo avere finito, fa tornare l'esecuzione all'indirizzo 0x8054327.

In questo momento lo stack è composto, dall'alto in basso, dai buffer interni e dalle variabili della funzione, da 32 bit di registro EBP e da 32 bit di indirizzo di ritorno. Lo stack contiene ancora gli argomenti passati alla funzione, ma la cosa non è di interesse per un aggressore.

L'indirizzo di ritorno, come già visto, è 0x8054327. Appena viene chiamata la funzione, si ritrova automaticamente immagazzinato nello stack. È questo indirizzo il punto debole, che può essere sovrascritto in modo che punti a una qualsiasi altra area di memoria in caso di overflow.

In un prossimo articolo affonderemo l'attacco vero e proprio.

Beth
i5b3773r@mac.com

SP2 RIMEDIA, MA...

All'indirizzo http://www.us-cert.gov/cas/techalerts/TA04-260A.html si trova la descrizione completa di una tipica vulnerabilità da buffer overflow in Windows. Se viene visualizzata una immagine JPEG creata ad arte da un aggressore, quest'ultimo può eseguire codice sul computer della vittima. Service Pack 2 protegge Windows, ma non le applicazioni; se una di queste installa sul PC una versione vulnerabile di gdiplus.dll, si è a rischio.

◄ *Se l'acqua trabocca, in inglese è overflow.*

Spy Shopping

Siamo andati su Internet a cercare equipaggiamento da spie. Ecco che cosa abbiamo trovato.

Questi oggetti li può comprare chiunque, con una carta di credito o prepagata, basta che sia accettata dai vari siti. Qualcuno spedisce anche contrassegno!

Videosorveglianza via cellulare

Il kit, composto da un server video e dalle telecamere necessarie, permette di ricevere immagini via telecamera direttamente su un cellulare GPRS abilitato Java.

spiare.com

139 euro, http://www. spiare.com/ videosorveglianza_mobile.html

Microfono da muro

Non è un microfono qualsiasi! Questo ascolta attraverso pareti fino a 70 centimetri di spessore. È grande più o meno come un pacchetto di sigarette e pesa 115 grammi inclusa batteria. La ditta spedisce anche contrassegno. Prezzo non disponibile, http://www.endoacustica.com/dettagli_mms_300.htm

Videoregistratore digitale

Questo apparecchietto da 11 centimetri contiene un hard disk da 40 giga, in grado di registrare fino a 80 ore di filmato video, oppure 600 ore di audio stereo (duemila ore di MP3!). Si attacca a un computer con porta USB. Prezzo non disponibile, http://www.spystore.it/schede/dvr80.htm

LA DOGANA

Internet è senza frontiere ma i doganieri non ci credono. Per i prodotti che arrivano da fuori Unione Europea ci saranno da pagare a parte l'IVA e il dazio doganale, in misura variabile secondo mille fattori.

MAGARI USATO

Andare su eBay e sui mille altri mercatini dell'usato online è un'ottima soluzione per trovare materiale da spionaggio a buon prezzo. Per fare un indirizzo dei tanti, http://www.mercatinoweb.com.

Molto spesso le immagini dei mercatini sono marchiate con il nome del sito, per evitare abusi. A tutti noi fa solo comodo sapere quali sono i siti, quindi ben venga la marchiatura.

Trasmittente ambientale nascosta nella calcolatrice

Costa, ma vale. Grazie a una potenza di emissione di sei milliwatt tira fino a cento metri in ambienti chiusi e 150 metri in campo aperto, con un'autonomia media di 72 ore (due batterie da 1,5 volt).
470 euro, http://www.selavio.com/home.html

Telecamera senza fili con audio nascosta nello stereo portatile

Ti credono un bulletto di strada e intanto registri. Tra la telecamera e il ricevitore possono esserci anche 300 metri, 500 metri nella versione potenziata.600 euro, http://www.dseitalia.it/Prod9.htm

Il sito Spygear.net vende attrezzature da spia per dodicenni o giù di lì. Sono prodotti in qualche modo limitati nella potenza ma perfettamente funzionali da tutti gli altri punti di vista. Occhiali per la visione notturna, sensori di movimento, metal detector: c'è veramente di tutto. Vale la pena dare un'occhiata.

SPIE MINI MA NON TANTO

Qualche estratto dal catalogo Spy Gear recuperabile presso http://spygear.net/index.php:

SPY WRIST CAM	Fotocamera digitale da polso	15 dollari
SPY LINK	Cuffie walkie-talkie	20 dollari
SPY CODE LAUNCHER	Lanciamessaggi con carta commestibile	10 dollari
SPY LISTENER	Occhiali da sole con microdispositivo di ascolto	15 dollari
SPY NIGHT SCOPE	Binocolo per visione notturna	15 dollari
SPY BINOCS	Vedere dietro sé senza essere visti	15 dollari
SPY METAL DETECTOR	Cercametalli da bambino	20 dollari
SECRET CAMERA JOURNAL	Diario con fotocamera nascosta	20 dollari
SNOOPPROOF SAFE	Cofanetto con antifurto a sensore di movimento	20 dollari
WRIST TALKIES	walkie-talkie da polso	15 dollari

Ed è solo l'inizio!

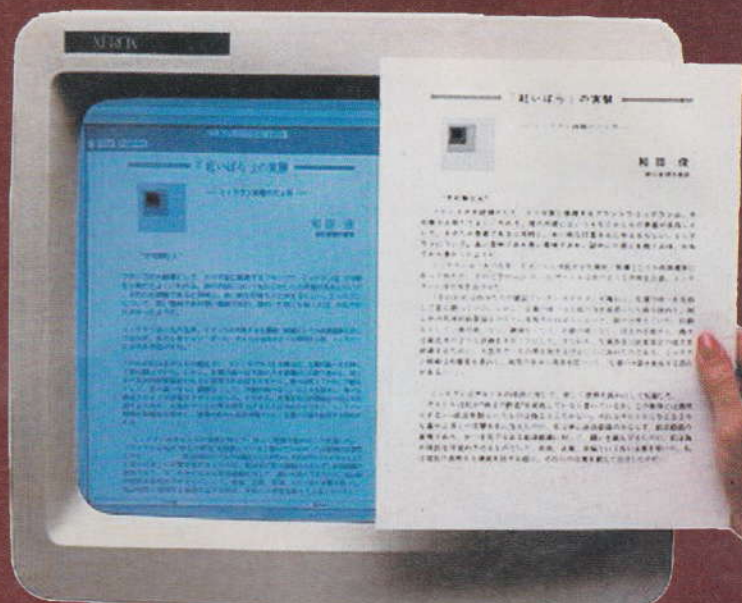
MA E' LEGALE?

In Italia non esiste una legge sullo spionaggio elettronico. Esistono la ben nota legge 675/1996 sulla tutela della privacy e c'è la legge 98 del 1974 che tratta genericamente l'uso di apparecchiature per monitoraggi. In sostanza, acquistare un oggetto come quelli presentati è del tutto legale; se l'utilizzatore ne fa un uso che viola qualche legge, è sua responsabilità.

Tutti i siti citati conducono a un elenco di prodotti ben più vasto di quelli presentati. Torneremo in argomento presto con altro equipaggiamento da spia!

Reed Wright
reedwright@mail.inet.it

FONDIAMO il C con l'HTML

Eccoci alle prese con un editor wysiwyg: un sistema di per sé facile. Crearlo lo è un po' meno

▲ Wysiwyg: esattamente ciò che vedi è ciò che ottieni. Bella roba.

Abbiamo già sentito parlare di editor html wysiwyg (What You See Is What You Get, letteralmente quello che vedi è quello che ottieni), vero? Dobbiamo anche sapere che stiamo parlando di editor comunissimi, come FrontPage, che ci scrivono il codice di una pagina html, mentre noi ci divertiamo a fare il drag-and-drop di immagini e a scrivere testi come fossimo in Word (o AbiWord o WordPad o qualunque text editor con formattazione).

Il codice originale

Da questo articolo impareremo come far interagire due linguaggi di programmazione, con una tecnica piuttosto originale (che qualcuno potrebbe definire perfino bizzarra), che fa un uso massiccio di alcune API, procedure ed elementi tipici delle console, senza altri commenti inutili.

Punto 1: Il Callback

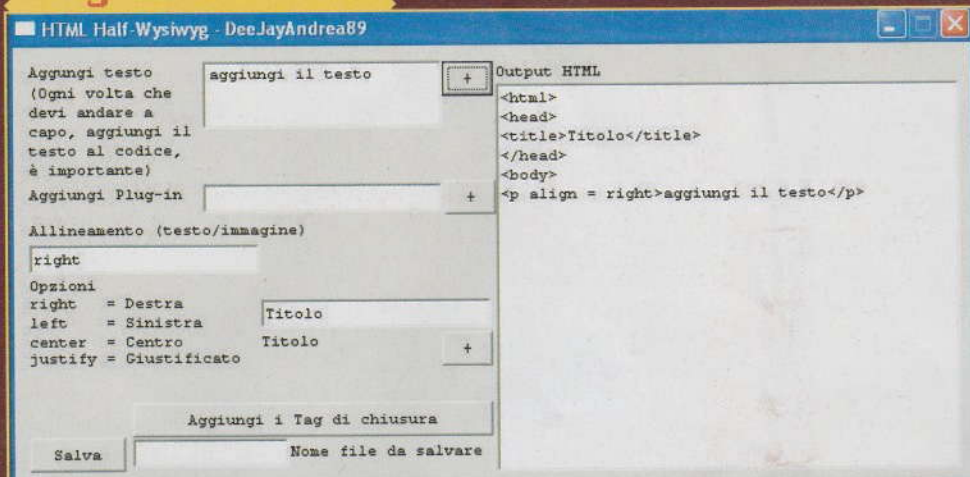
Più che altro del callback serve il concetto. È un'operazione compiuta non dal programma, quanto dal sistema operativo stesso.

Punto 2: Il Main

Anche il codice del main (anzi APIENTRY WinMain) è poco influente sul codice del resto del programma, ma per fare in modo che l'eseguibile giri senza intoppi bisogna impostarlo così. Per ci; di cui parliamo in questo articolo non è la parte più interessante, ma il codice è quello.

Figura 1.

▲ Se non inseriamo il titolo, ci apparirà questa fastidiosa finestra.

Figura 2.

▲ *Se invece lo inseriamo, nessuna finestra si aprirà per darci fastidio.*

Punto 3: Il buffer HTML e il salvataggio

Abbiamo chiamato così il buffer che raccoglie di volta in volta il codice html e ce lo scrive sullo schermo. Il buffer in questione verrà scritto su un file (del quale dobbiamo inserire il nome nel campo apposito) al termine delle modifiche. Se non sappiamo cos'è il buffer: è una variabile che funge da contenitore di dati, può essere utilizzato infinite volte e ci permette di non allocare memoria. Il nostro buffer html è una stringa alla quale vengono appese di volta in volta stringhe formate da una parte fissa (il tag) e da una variabile (testo, nome file, plugin, allineamento).

Punto 4: Il Titolo

Questo è particolare. La variabile "tit" viene inizializzata, cioè le viene assegnato il valore predefinito "falsetitle". Perché? Per prevenire errori di tag. Prima di tutto viene chiesto il titolo, così il programma può appendere in testa alla stringa i tag di apertura della pagina html.
Guardiamo le figure 1 e 2. Se il titolo non è stato inserito nel campo, e quindi "tit" è sempre uguale a "falsetitle", il programma manda un messaggio di errore e ritorna 1 (chiude la procedura e torna in modo di attesa), altrimenti a "tit" viene sovrascritto il valore inserito, allora non si possono più verificare messaggi d'errore circa il titolo. I primi tag sono inseriti (fig. 2) e ora possiamo aggiungere il testo e/o la plug-in. Notiamo che la condizione del testo vale per qualunque campo d'inserimento.

Punto 5: Aggiunta testo da tastiera

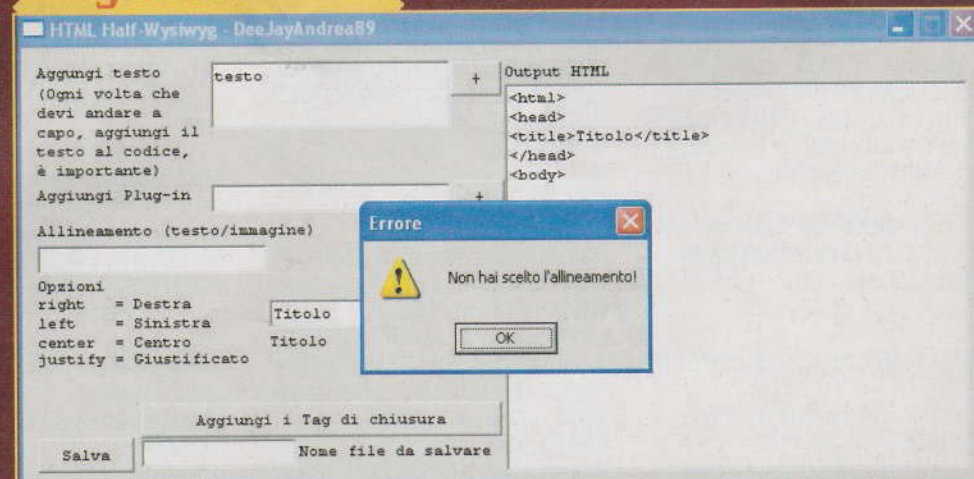
Qui viene inserito il testo dalla tastiera. Alcune precisazioni. Per fare in modo che il testo venga visualizzato a capo nel browser, bisogna aggiungere i tag necessari (col pulsante "+" del campo testo, non ci si può sbagliare, è lì accanto) e allora il buffer temporaneo (che viene usato per i campi temporanei e modificabili, cioè il testo e le plug-in) denominato "tmpbuff" viene svuotato e il testo del campo di inserimento testo (lo so è ridondante, ma non c'è verso di dirlo diversamente) viene settato come questo buffer quindi, essendo il buffer vuoto, anche il campo di testo risulterà vuoto, pronto per scriverci sopra. I campi fissi (Titolo e nome file) non usano buffer temporaneo, perché una pagina html può avere uno e un solo titolo, così un file può avere uno e un solo nome.
Un avvertimento: dobbiamo _per forza_ inserire un allineamento, le opzioni sono scritte sotto il campo stesso, altrimenti avremo un altro errore. Provare per credere: figura 3.

Punto 6: Aggiunta di plug-in da file

Questo è molto semplice: indichiamo la directory del file che vogliamo inserire e clicchiamo sul "+" e al buffer html verranno appesi i tag per le plug-in (<embed src =...), e il nome file.
Se, per esempio, abbiamo un gioco Flash che vorremo inserire, di nome foo.swf, dovremo solo digitare foo.swf (se il file .swf si troverà nella stessa directory della pagina HTML, altrimenti dobbiamo inserire il percorso preciso es. se il file.swf sarà nella cartella foo, dovremo digitare foo/foo.swf) e cliccare sull'ormai famoso "+" per inserire al volo i tag.

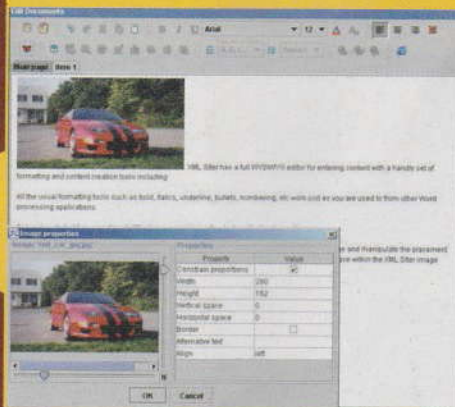
Punto 7: Aggiunta tag di chiusura

Abbiamo finito di inserire tutti i tag? Un clic su "Aggiungi i Tag di chiusura" e di nuovo il campo del codice html si

Figura 3.

▲ *La stessa cosa vale per l'allineamento. La finestrella fastidiosa ha solo un contenuto differente.*

aggiornerà. Notiamo che i tag di chiusura non sono affidati a un buffer, perché sono costanti: infatti al buffer html è appesa una stringa che non fa riferimento a una variabile, bensì puro testo delimitato da “virgolette”.

Punto 8: Il salvataggio

Apportiamo a mano le ultime modifiche al codice html dal campo apposito (se necessario) e poi scegliamo la directory di salvataggio e un nome da inserire accanto al pulsante “Salva”. Mi raccomando, anche l'estensione! Ecco finalmente la nostra pagina html pronta per la visualizzazione con Mozilla o Opera o Netscape o quanto altro. Abbiamo finito!

Un editor wysiwyg completo permette di creare pagine web in un batter d'occhio.

Punto 9: Inizializzazione

Finora abbiamo trattato i moduli del programma, non l'esecuzione. Ecco, questa parte è un altro modulo: quando e dove viene caricato lo vediamo dopo. Questa parte è utilissima perché ci permette di settare parametri base e inizializzare buffer. Qui vediamo l'API SendDlgItemMessage, in questo caso settiamo il numero massimo di lettere inseribili in un campo (EM_SETLIMITTEXT).

Questo campo è l'allineamento: viene usato per questo un array di 9 char, poiché l'allineamento che si scrive con più parole di tutte è “justify”, che occupa 8 caratteri. Quindi in piena regola.

Il testo massimo viene settato perché altrimenti qualcuno potrebbe inavvertita-

IL CODICE SORGENTE

SUL PROSSIMO NUMERO DI HACKERS MAGAZINE TROVEREMO QUESTO CODICE E ANCHE ALTRI FILE UTILI

```
//Half WYSIWYG - Quasi editor HTML
//quello che vedi non è proprio quello che ottieni, però...
#include <windows.h>
#include <windowsx.h>
#include <commctrl.h>
#include <string.h>
#include <stdio.h>
#include “wysiwyg.h”

//Definizione callback. cfr. Punto 1
static BOOL CALLBACK DialogFunc(HWND hwndDlg, UINT msg, WPARAM wParam, LPARAM lParam);

//Main. cfr. Punto 2
int APIENTRY WinMain(HINSTANCE hinst, HINSTANCE hinstPrev, LPSTR lpCmdLine, int nCmdShow)
{
        WNDCLASS wc;
        INITCOMMONCONTROLSEX cc;

memset(&wc,0,sizeof(wc));
        wc.lpfnWndProc = DefDlgProc;
        wc.cbWndExtra = DLGWINDOWEXTRA;
        wc.hInstance = hinst;
        wc.hCursor = LoadCursor(NULL, IDC_ARROW);
        wc.hbrBackground = (HBRUSH) (COLOR_WINDOW + 1);
        wc.lpszClassName = “wysiwyg”;

RegisterClass(&wc);

memset(&cc,0,sizeof(cc));
        cc.dwSize = sizeof(cc);
        cc.dwICC = 0xffffffff;
        InitCommonControlsEx(&cc);

        return DialogBox(hinst, MAKEINTRESOURCE(IDD_MAINDIALOG), NULL, (DLGPROC) DialogFunc);

}

FILE *fp;
static char fname[1024];
static char tmpbuff[65535];
static char htmbuff[65535] = “”; //Buffer HTML e inizializzazione, cfr. Punto 3
static char align[10];
static char plg[256];
static char tit[1024] = “falsetitle”; //Inizializzazione titolo. cfr. Punto 4.1

//Aggiunta titolo, cfr. Punto 4
static int titolo(HWND hwnd)
{
    //Per la seguente condizione, cfr. Punto 4
        if(strnicmp(tit, “falsetitle”, 10)) {
            //Punizione!
            MessageBox(hwnd, “Inserisci un titolo!”, “Messaggio”, MB_OK | MB_ICONWARNING);
            return 1;}
        else {
GetDlgItemText(hwnd, IDTITLE, tit, sizeof(tit));
        strcat(htmbuff, tit);
        strcat(htmbuff, “</title>\r\n</head>\r\n<body>\r\n”);
SetDlgItemText(hwnd, IDHTMOUT, htmbuff);
        return 0;}
}
//Aggiunta testo da tastiera, cfr. punto 5
static int addtext(HWND hwnd)
{
        //Per la seguente condizione, cfr. Punto 4
        if(!strnicmp(tit, “falsetitle”, 10)) {
            MessageBox(hwnd, “Inserisci un titolo!”, “Messaggio”, MB_OK | MB_ICONWARNING);
            return 1;}
        else {
GetDlgItemText(hwnd, IDALIGN, align, sizeof(align));

if(GetDlgItemText(hwnd, IDALIGN, align, sizeof(align))==0) {

MessageBox(hwnd, “Non hai scelto l'allineamento!”, “Errore”, MB_OK | MB_ICONWARNING);
            return 1;}
        strcat(htmbuff, “<p align = “);
        strcat(htmbuff, align);
        strcat(htmbuff, “>”);

GetDlgItemText(hwnd, IDINTXT, tmpbuff, sizeof(tmpbuff));
        strcat(htmbuff, tmpbuff);
        strcat(htmbuff, “</p>\r\n”);

SetDlgItemText(hwnd, IDHTMOUT, htmbuff);
        strcpy(tmpbuff, “”); //Puliamo il buffer
```

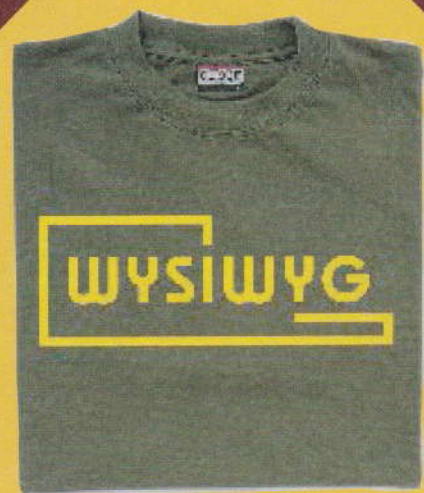
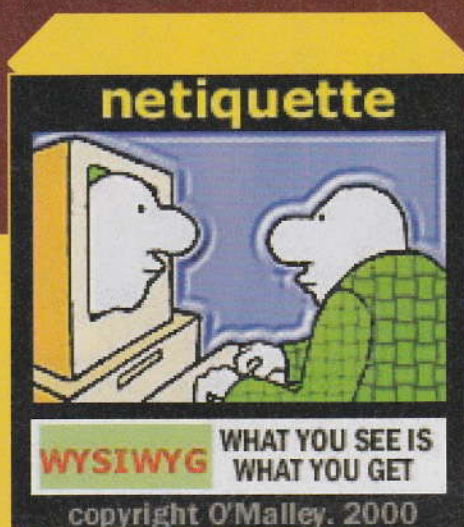
mente digitare"justifyyyyy", che occupa più di 9 caratteri, quindi si otterrebbe un buffer overflow (se il buffer trabocca, anche di un solo carattere, il programma si pianta). Al buffer html (già inizializzato con zero caratteri: static char htmbuff[65535] = "";) sono appesi i tag iniziali, che saranno settati a schermo nel campo dell'output html al momento dell'aggiunta del titolo.

netiquette

WYSIWYG WHAT YOU SEE IS WHAT YOU GET

copyright O'Malley. 2000

Punto 10: Esecuzione del Callback

Ecco il clou del programma! La variabile "msg" viene sottoposta a "case": a seconda del pulsante premuto, o dell'evento accaduto, vengono restituite in output le varie funzioni. WM_INITDIALOG (quando si apre il dialogo, cioè il programma) avvia InitializeApp (Inizializzazione dell'applicazione, appena analizzata), e funziona sempre. Poi abbiamo WM_COMMAND, con un altro "case" annidato che gestisce gli elementi visuali (pulsanti, combo-box, edit-box, check-box ecc.): alla pressione del tal pulsante fai questo, se clicchi quel pulsante fai quell'altro eccetera.
È da qui che vengono chiamate tutte le funzioni analizzate finora. WM_CLOSE (EndDialog(hwndDlg,0);) rappresenta la pressione della "X" rossa in alto a destra. Alla fine di tutto, il programma ritorna FALSE.

DeeJayAndrea89
THA POWAH OF SOUND!

```
temporaneo...

SetDlgItemText(hwnd, IDINTXT, tmpbuff);
        return 0;}
}

//Aggiunta plug-in da file, cfr. Punto 6
static int addplg(HWND hwnd)
{
        //Per la seguente condizione, cfr. Punto 4
        if(!strnicmp(tit, "falsetitle", 10)) {
                MessageBox(hwnd, "Inserisci un titolo!", "Messaggio", MB_OK | MB_ICONWARNING);
                return 1;}
        else {

GetDlgItemText(hwnd, IDINIMG, img, sizeof(img));
        strcat(htmbuff, "<embed src = \"");
        strcat(htmbuff, img);
        strcat(htmbuff, "\">");

SetDlgItemText(hwnd, IDHTMOUT, htmbuff);
        strcpy(img, "");

SetDlgItemText(hwnd, IDINIMG, img);
        return 0;}
}

//Aggiunta dei tag finali. cfr. Punto 7
static int closetag(HWND hwnd)
{
        //Per la seguente condizione, cfr. Punto 4
        if(!strnicmp(tit, "falsetitle", 10)) {
                MessageBox(hwnd, "Inserisci un titolo!", "Messaggio", MB_OK | MB_ICONWARNING);
                return 1;}
        else {
        strcat(htmbuff, "</body>\r\n</html>");

SetDlgItemText(hwnd, IDHTMOUT, htmbuff);
        return 0;}
}

//Salvataggio file, cfr. Punto 3 e Punto 8
static int salva(HWND hwnd)
{

GetDlgItemText(hwnd, IDFNAME, fname, sizeof(fname));
        fp = fopen(fname, "w");
        GetDlgItemText(hwnd, IDHTMOUT, htmbuff, sizeof(htmbuff));
        fprintf(fp, "%s", htmbuff);
        fclose(fp);
        return 0;
}

//Inizializzazione dell'applicazione, cfr. Punto 9
static int InitializeApp(HWND hwnd,WPARAM wParam, LPARAM lParam)
{
        SendDlgItemMessage(hwnd, IDALIGN, EM_SETLIMITTEXT, 9, 0);
        strcat(htmbuff, "<html>\r\n<head>\r\n<title>");
        return 0;
}

//Esecuzione del callback, cfr. Punto 10
static BOOL CALLBACK DialogFunc(HWND hwndDlg, UINT msg, WPARAM wParam, LPARAM lParam)
{
        switch (msg) {

        case WM_INITDIALOG:
                InitializeApp(hwndDlg,wParam,lParam);
                return TRUE;

        case WM_COMMAND:
                switch (LOWORD(wParam)) {

case IDOK:

salva(hwndDlg);

return 1;

case IDADD:

addtext(hwndDlg);

return 1;

case IDADDIMG:

addimg(hwndDlg);

return 1;

case IDTITLE:

titolo(hwndDlg);

return 1;

case ID_CLSTAG:

closetag(hwndDlg);

return 1;
                }
                break;

        case WM_CLOSE:

EndDialog(hwndDlg,0);
                return TRUE;

        }
        return FALSE;
}
```

Primi Titanici

Quanto è grande un numero grande e come diventare famosi scoprendone uno!

La matematica è noiosa solo a scuola. Fuori c'è un sacco da divertirsi soprattutto se abbiamo un computer in mano e una mentalità hacker nella testa!

Per esempio, è noto che i moderni sistemi di cifratura a chiave pubblica si basano sulla generazione di numeri enormi e sulla difficoltà di recuperare i fattori che hanno generato il numero in questione.

Quindi trovare numeri primi sempre più grandi è di importanza fondamentale. Li chiamano numeri primi titanici e chi li trova può anche acquisire un pizzico di notorietà!

Fama (e soldi?) con i titanici

Al momento il numero più titanico di tutti è un mostro: 2^24036583-1. Scritto cifra per cifra ci vorrebbero quindici numeri di Hacker Journal per contenerlo tutto! Lo ha scoperto Josh Findley lo scorso 15 maggio. Josh Findley non è un matematico né un ricercatore; è un ragazzo come tanti, che però ha installato un programma apposta per effettuare la ricerca.
Ha avuto pazienza, elaborando dati per più di cinque anni, ma ce l'ha fatta. Ci vuole anche un pizzico di fortuna: la scoperta ha infatti richiesto solo un paio di settimane su un Pentium 4 a 2,4 GHz. Diventerà molto più famoso quello che domani scoprisse segnali di vita intelligente con Seti@Home... ma questa ricerca è più utile.

Quanti scoprono un primo titanico appaiono nel database all'indirizzo http://primes.utm.edu/bios/index.php. Come fare? Si scarica il client all'indirizzo http:// mersenne.org/freesoft.htm (ci sono per tutti i sistemi, da Windows a Linux a Mac OS X) e lo si fa andare il più possibile.

Qualcuno molto fortunato potrebbe perfino farci dei soldi. La Electronic Frontier Foundation ha istituito un premio di centomila dollari per chi batterà sul tempo tutti nel trovare un numero primo più grande di dieci milioni di cifre! Ci sono anche premi superiori, ma ci vorrà tempo. Tutto è spiegato su http://www.eff.org/awards/ coop.html.

Perché non mettersi a cercare titanici? Potrebbe essere utile e sicuramente c'è da scoprire qualcosa di nuovo!

P. Greco
p.greco@hackerjournal.it

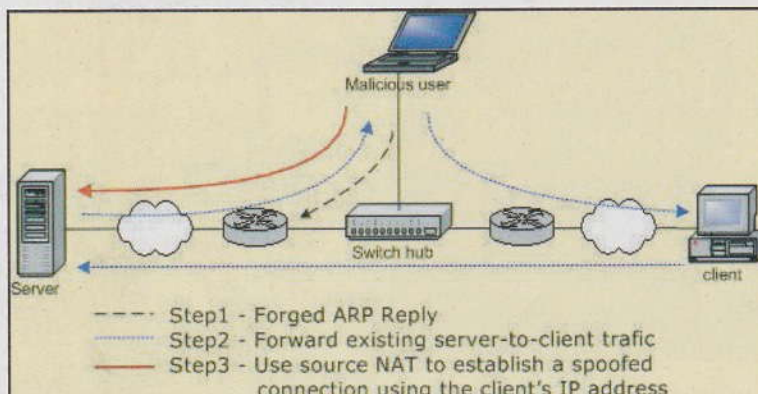
L'ENIGMA DELLA FATTORIZZAZIONE

Se abbiamo due numeri primi un po' grandi, come 1000000000000000357 e 1000000000000000709, moltiplicarli è fastidioso ma non è tanto difficile; con un po' di pazienza lo si può fare anche a mano (quanto fa?). Ma avendo il numero 1000000000000001066000000000000253113, come si fa a capire quali sono i numeri da moltiplicare per ottenerlo? I programmi di cifratura a chiave pubblica si basano su questo principio e quindi trovare numeri primi sempre più grandi è di importanza altrettanto grande ai fini delle tematiche di cifratura. Se i numeri non sono primi, tutto il castello cade, ed è altrettanto difficile capire se un numero è primo o meno. Un numero primo, per chi l'ha scordato, è divisibile solo per 1 e per sé stesso. Il primo numero primo è 2. Chi conosce altre proprietà interessanti sui numeri primi?

▲ *Marin Mersenne, 1588-1648. Una volta i cercatori di numeri primi si nascondevano nei monasteri.*

ENCICLOPEDIA dell'Hacking!

Spoofing

La tecnica di bloccare, alterare e ritrasmettere un flusso di comunicazione ingannando il destinatario rispetto alla propria identità. In particolare l'IP spoofing varia gli indirizzi TCP/IP o li maschera nell'intestazione del pacchetto.

ESEMPIO

Esistono diverse tecniche di spoofing, cieco(blind) e non cieco. Nel secondo caso l'attaccante cerca di prendere l'identità di un altro host presente nella sua sottorete, vedendo i pacchetti che sono indirizzati anche agli altri computer. Nel caso cieco, cerca di farsi passare per un host qualunque anche se non è della sua sottorete, ma di conseguenza può solo cercare di indovinare il numero di sequenza che lo potrebbe far passare per l'host mittente.

man-in-the-middle
I pacchetti sono sniffati da un collegamento tra i due punti della trasmissione. Si può fare in modo di diventare la destinazione finale.

routing redirect
Una specifica forma di attacco man-in-the-middle che redirige le informazioni di routing dall'host originale all'host dell'hacker.

source routing
Redirigere singoli pacchetti tramite l'host dell'hacker

blind spoofing
Si predicono le risposte dell'host attaccato inviando i comandi, la cui risposta però non si può ricevere perché sarà inviata all'host che si impersonifica.

flooding
Una serie di pacchetti SYN del protocollo TCP/IP vengono spediti in un breve lasso di tempo . Il server che li riceve non fa in tempo a liberare le risorse necessarie alle connessioni e il sistema risulta, di fatto, impossibilitato a funzionare. E' quindi anche un tipo di attacco DOS (denial of service).

IP SPoofing Attacks and

Hijacked Terminal Connections

CERT Advisory CA-95:01

Das DFN-CERT Team der Universität Hamburg

Ein zweiter brandaktueller Beitrag beschäftigt sich mit dem Thema "Network Security". Auf einer Konferenz in den USA (CMA
über diese Art des Angriffes auf seine Rechner geschildert. Unter der Leitung des CERT Coordination Centers wurde das nachfo

!!! Nuke & Spoofer !!!

X ident	Discreto Ip-Spoofer che permette il settaggio di altre interessanti impostazioni...
[illegible]	Ottimo Ip-Spoofer
[illegible]	Programma nuke che consente di nukare + ip contemporaneamente!
Internet Maniac	Ping - flood - spoof ecc......
[illegible]	ottimo smurf
[illegible] Generator 0.85	buon programma che genera vari tipi di attacchi, tra cui lo smurf
VClone	nuker che sfrutta i cloni
[illegible]	Ottimo programma che funge da : flooder, nuke ecc...
[illegible] nuke 2.5	nuke con tante funzionalità
[illegible]	semplice nuker
WinSpoof	Programma per navigare anonimo spoof(ando (nascondendo) il tuo ip!!!!!!

Requisiti

Conoscere il protocollo TCP/IP, come sono fatti i pacchetti IP e come avviene la connessione TCP.

Security

In particolare il flooding, molto di moda qualche anno fa, è pressoché inutilizzabile con i nuovi sistemi di sicurezza adottati da quasi tutti i server. Lo spoofing cieco per ottenere pieno successo deve saper prevedere il sequence number dei singoli pacchetti. Se, come nei recenti kernel Linux, la generazione è pseudocasuale, difficilmente si riesce a predirli. L'installazione di un firewall può impedire alcuni di questi attacchi.

SHIMOMURA DESCRIVE I DETTAGLI TECNICI DI COME KEVIN MITNICK USÒ L'IP SPOOFING PER ENTRARE NEL SUO SISTEMA:
http://www.gulker.com/ra/hack/tsattack.html

PER SAPERNE DI PIÙ:
http://sugwww.uni-paderborn.de/suginfo/1.95/1.95_ipattack.html

PER QUALCHE PROGRAMMA DA STUDIARE:
http://www.ultrasonik.it/programmi.htm

ENCICLOPEDIA dell'Hacking!

Phreaking

HACKING DEL SISTEMA TELEFONICO. LA MAGGIOR PARTE DELLA LETTERATURA E DELLE TECNICHE CHE SI TROVANO IN GIRO SONO APPLICABILI A SISTEMI TELEFONICI DI CIRCA VENT'ANNI FA.
I MODERNI SISTEMI TELEFONICI SONO DIFFICILMENTE ATTACCABILI E DA QUANDO L'ELETTRONICA PROGRAMMABILE È DIVENTATA L'UNICA VIA PER GESTIRE LE CENTRALI TELEFONICHE QUASI NESSUNA DELLE TECNICHE PASSATE PUÒ ANCORA FUNZIONARE.
LA CONOSCENZA DEL FUNZIONAMENTO DELLE CENTRALI TELEFONICHE, DI QUALUNQUE TIPO, È COMUNQUE UN BAGAGLIO CHE L'HACKER NON PUÒ TRASCURARE.
OGGI ABBIAMO DUE GRANDI FILONI CHE POSSIAMO UTILMENTE INDAGARE: QUELLO DELLA TELEFONIA FISSA E QUELLO DELLA TELEFONIA MOBILE. ESTENSIONI DI QUESTI TERRITORI D'ESPLORAZIONE SONO TUTTO L'AMBIENTE DELLE CARTE TELEFONICHE E DELLA LORO CODIFICA, SPESSO PROPRIETARIA E DIFFICILMENTE INTERPRETABILE.
CONOSCERE GLI IMPIANTI TELEFONICI INTERNI È UN ALTRO 'MUST': COME COLLEGARE UN TELEFONO, UN MODEM, COME METTERLI IN SERIE O AUTOESCLUDERLI E COSÌ VIA, FA PARTE DI UN PHREACKING DI BASSO LIVELLO, MA MOLTO UTILE IN TANTE OCCASIONI.

ESEMPIO

Quando si formano i numeri, sui moderni apparecchi telefonici un apposito chip genera dei toni di frequenze differenti che corrispondono al numero premuto e che sono riconosciuti dalla centrale. Una routine software sperimentale, per fare la stessa cosa su pc, può essere questa:

```
DTMF in C (on a PC) by Kirk Hobart
#include  stdio.h
#include  ctype.h
#include  math.h
#include  conio.h

#define BITS 0xFF00
#define NOISE 0           /* enable noi-
se shaper */
#define TON  0.100        /* tone dura-
tion */
#define TOFF 0.100       /* silence dura-
tion */
#define RAMP 0.002        /* tone rise
and fall time */
#define RATE 11025.0     /* sample rate
*/
#define                  numberof(n)
(sizeof(n)/sizeof(*n))

struct

  char letter;
  double f1, f2;
  button

    '1', 697, 1209  ,
    '2', 697, 1336  ,
    '3', 697, 1477  ,
    'A', 697, 1633  ,
    '4', 770, 1209  ,
    '5', 770, 1336  ,
    '6', 770, 1477  ,
    'B', 770, 1633  ,
    '7', 852, 1209  ,
    '8', 852, 1336  ,
    '9', 852, 1477  ,
    'C', 852, 1633  ,
    '*', 941, 1209  ,
    '0', 941, 1336  ,
    '#', 941, 1477  ,
    'D', 941, 1633  ,
    'X', 20,  20  ,
    'Y', 100,  100  ,
    'Z', 500,  500  ,
  ;

int main(void)

  double t, v  0;
  char c;
  int value  0, n;
  FILE *fout;

  puts("Press 123A456B789C*0#D to digi-
tize DTMF-tones to file. Fs  11025. ESC
quits.");
   fout   fopen("x", "wb");
  while (1)

    c   toupper(getch());
    if (c    0x1B)
      break;
    for (n  0; n  numberof(button); n     )

      if (c    button  n  .letter)

        putchar(c);
        for (t  0.0; t  TON; t     1/RATE)

          v    sin(2*M_PI*button  n  .f1*t)
    sin(2*M_PI*button  n  .f2*t);
          if (t   RAMP)        /* See Note
Below */
          v *   t/RAMP;        /* See Note
Below */
          if (t  TON-RAMP)     /* See Note
Below */
          v *   (TON-t)/RAMP; /* See Note
Below */
        #if NOISE
                              value
floor(v*(BITS/4)  BITS/2)   (value&  BITS);
        #else
        value    floor(v*16383  32768.5);
        #endif
        fputc((value&BITS)     8, fout);

      for (t  0.0; t  TOFF; t     1/RATE)
        fputc(0x80, fout);



  putchar('  n');
  fclose(fout);
  return 0;

          v *   (TON-t)/RAMP;
        #if NOISE
                              value
floor(v*(BITS/4)  BITS/2)   (value&  BITS);
        #else
        value    floor(v*16383  32768.5);
        #endif
        fputc((value&BITS)     8, fout);

      for (t  0.0; t  TOFF; t     1/RATE)
        fputc(0x80, fout);



  putchar('  n');
  fclose(fout);
  return 0;
```

Requisiti

Farsi una panoramica di come funziona un sistema telefonico è il primo passo, a partire dall'impianto telefonico di casa e dal local loop: il doppino che ci collega alla centrale più vicina, se già non siamo cablati con la fibra ottica.

Security:

Mai lasciare incustodito il proprio telefonino! ;)

Glossario dei termini telefonici: http://www.wordiq.com/definition/Glossary_of_telephony_terms
Un buon punto di partenza per capire la complessità di un sistema telefonico moderno: http://www.ericsson.com/support/telecom/part-a/index.shtml

Da staccare e conservare nel tuo raccoglitore

CIFRATURA ALLA RADICE: LE RISPOSTE!

CYBERENIGMA DI HACKER JOURNAL 58

Il diagramma di flusso di DUNE!

Le domande

Avevamo un cifrario a chiave composto solo da numeri tra 0 e 9 e un po' di disegnini, purtroppo stampati un po' piccoli, che suggerivano le risposte, consistenti in varie radici quadrate…

PER TUTTI: qual è la radice quadrata di 3? Quanti decimali riusciamo a trovare?
PER ESPERTI: il messaggio cifrato è TVITYJXUQWFIKIRDORDIXC-SIQWMSTLBTTTWXTPBVMK. la chiave è un cerchio con dentro tracciato il suo diametro.
PER GENI: il messaggio cifrato è VTPCNRGDMBYILQWU-CIWVTSYZKLLGLBJTWCOPAYGNWAZVHCBRT. La chiave è una spirale.
PER SUPER HACKER: scrivere un programma che calcoli la radice quadrata di un numero senza ricorrere a una istruzione specifica già pronta.

Le risposte

PER TUTTI: Su ftp://sailor.gutenberg.org/pub/gutenberg/etext96/3sqrt10.txt si trova un milione di decimali della radice di 3. Le radici di altri numeri sono a http://antwrp.gsfc.nasa.gov/htmltest/rjn_dig.html.
PER ESPERTI: il messaggio era QUESTAVOLTAABBIAMOVERAMENTEPRESOTROPPOSOLE. La chiave era 31415926535897932384626433832795 0288419716, ossia pi greco, ossia il rapporto tra il cerchio e il suo diametro.
PER GENI: il messaggio era UNOUNODUETRECINQUEOTTOTREDICIVENTUNOTRENTAQUATTRO. 1, 1, 2, 3, 5, 8, 13, 21, 34… la serie di Fibonacci, che tende al numero phi, equivalente a 16180339887498948482045868343656 38117720309179805 (manca la virgola, ovvio), con cui si può disegnare la spirale aurea.
PER SUPER HACKER: http://www.qnet.fi/abehr/Achim/Calculators_SquareRoots.html, oltre a molti altri siti, spiega come calcolare una radice quadrata usando solo carta e matita.

Chi ha risposto!

PER TUTTI

Matteogeniaccio, otto decimali (ma anche super hacker); Luca Betti, 31 decimali; R3b3l, cinque decimali; m3t4lup (DIECIMILA decimali e dopo ha mandato anche il programma da super hacker); MORONCELLI FEDERICO, 31 decimali.

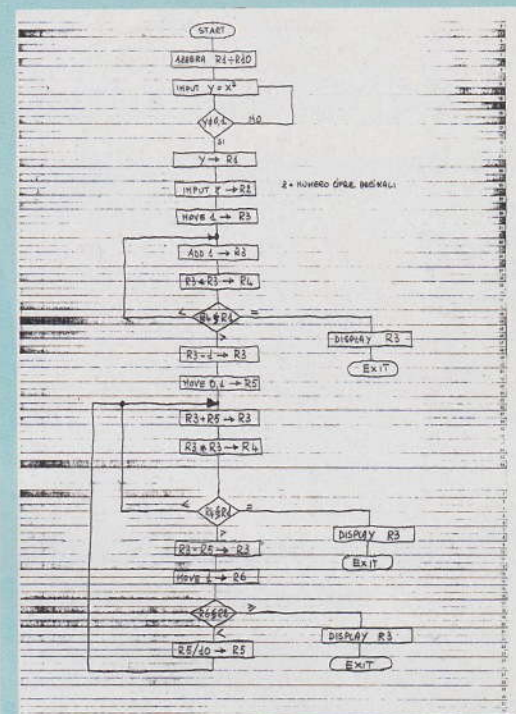
PER ESPERTI

Valkiry (ottimo).

PER GENI

Kinslayer (ok); Samwise (con 31 decimali di radice di 3, attendiamo il programma); Enrico Sunseri, con quattordici decimali di radice; YANEZ E FABIANO (saluto speciale a Yanez!).

SUPER HACKER

figlioccio81, Java, primo arrivato! Gianluca Ghettini, C; ThN1saHead, Visual Basic; Matteogeniaccio, Visual Basic; OOsiris, C++; Scopel, Python; JimB0Th, PHP, jimb0th@cappellin.net, http://www.cappellin.net/modules.php?name=SquareRoot. E ha risposto a tutti i quesiti, con cento decimali della radice di 3. Bravissimo; AlexMark, C++; -._.·´¯`·._.-´(EaglE)`-._.·´¯`·._.-, Turbo Pascal (15 anni, complimenti); -=Lyonard=-, Javascript e sedici decimali della radice di tre (TheGuilty ringrazia!); Io & Heike, VB.NET; kal_el1965, C; exKaPe, C, exkape@tele2.it; JOE, VB, dedicato al suo amore Chia (Chia, tientelo stretto, ha un sacco di buoni algoritmi!!!); E g i X, VB; FTP21, VB; 13c0lp1, Java; Poia87, VB; Teorema55, Javascript; snakeblu, VB (e 14 decimali); roy20021, Pascal (li pubblichiamo su Hackers Magazine, i codici! Il tuo codice non è male, bravo); a.renzi, Pascal; Daniele Midi, VB e 31 decimali; Black Hawk, VB6, 15 anni e UN MILIONE di decimali; m3t4lup, C; Torculus, Java, proprio ben fatto; Cancel, Python; D4re_Dev1l, Excel e VB (più decimali a piacere); CyberPunk, C; cripto, C; MaNetTa®, C; yayo, PHP; VERNAM, Java; Mauro Barzaghi, Java; gas_73, Java; .:LoZ:., PHP; snakeblu, VB; GeminiNero, Fortran90; Salvatore, C; DUNE, flowchart (eccezionale!); il pirata felice, VB; DiOne, VB; Francesco, VB.NET; ipOt, C++; Ezio Rizzo, QBasic 4.5.

Al prossimo cyberenigma!

CYBERENIGMA

PALLA DI CRISTALLO!

Abbiamo chiesto a un hacker medium (non large!) di guardare nel futuro. Ha detto Unix e ha visto una data, ma la sua visione era un po' confusa... la visione era questa:

ABBIAMO CAPITO CHE È UNA DATA DELICATA PER UNIX, MA POCO ALTRO.

✪ Per tutti: qual è la data? É ancora lontana, ma dicevano così anche del 2000 quando è nato il DOS...
Domanda grafica: come si chiama una immagine come quella sopra?
✪✪ Per esperti: che cosa succederà a Unix in quella data?
Domanda grafica: ci sono siti che spiegano come produrre queste immagini? E programmi?
✪✪✪ Per geni: quali sono le date corrispondenti per Windows e Macintosh?
Domanda grafica: sei capace di produrre un'immagine come questa? Magari con dentro la data opposta a quella di questa immagine?
✪✪✪✪ Per super hacker: sai produrre una immagine come questa con un programma? Le più belle le pubblichiamo (ma vogliamo il programma)!
Domanda grafica, super difficile: sai scrivere un programma per decodificare questa immagine?

Arrivederci al prossimo cyberenigma!

le risposte a:

guestbook@hackerjournal.it